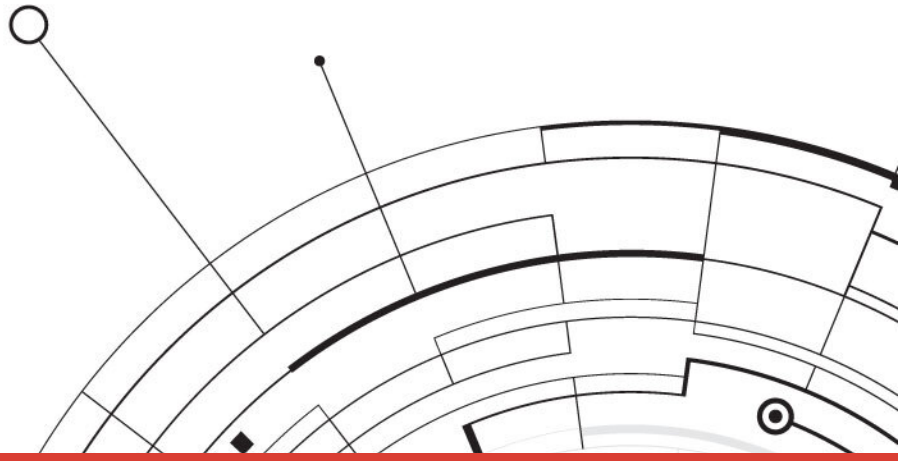
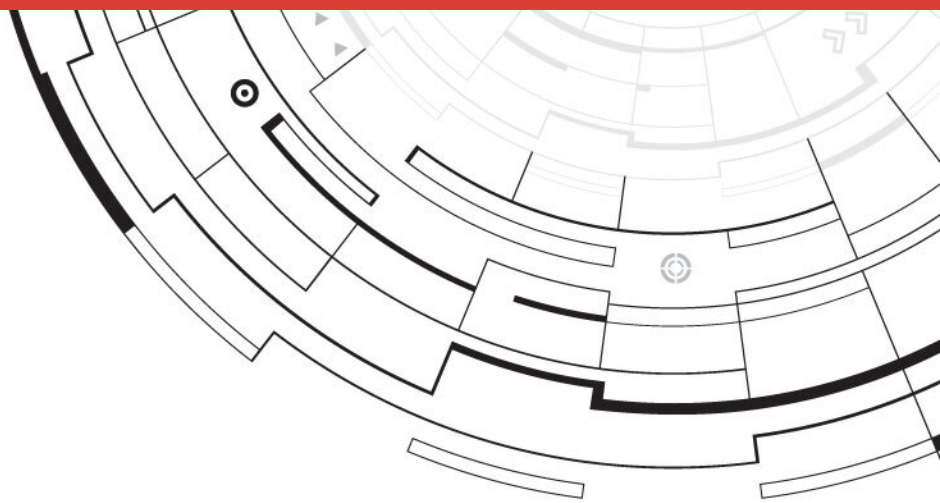
vPENTEST



Internal Network Penetration Test

VULNERABILITY REPORT



Demo Client

June 06, 2021

app.vpentest.io

vPENTEST

Copyright

Confidentiality

This document contains company confidential information of a proprietary and sensitive nature. As such, this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only and should not be copied without written permission. vPenTest Partner treats the contents of a security audit as company confidential material and will not disclose the contents of this document to anyone without written permission.

Assessment Project Team

Below is a list of contacts that were involved on this engagement. Should you have any questions pertaining to the content of this document or any project and non-project related items, please feel free to reach out to the necessary project contacts.

Primary Point of Contact	
Name:	Demo Consultant
Title:	Consultant
Mobile:	+1(504) 507-0558
Office:	+1(844) 866-2732
Email:	altonjx@gmail.com

Discovered Vulnerabilities

The following table displays a summary of the vulnerabilities that were discovered as part of this engagement.

DISCOVERED VULNERABILITIES	THREAT SEVERITY RANKINGS	
Internal Network Security Assessment (129)		
AXIS HTTP GET Heap Overflow	Critical	
AXIS Multiple Vulnerabilities (ACV-128401)	Critical	
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	Critical	
Microsoft SQL Server Unsupported Version Detection (remote check)	Critical	
Microsoft Windows XP Unsupported Installation Detection	Critical	
MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	Critical	
Unix Operating System Unsupported Version Detection	Critical	
Unsupported Windows OS (remote)	Critical	
VMware ESX / ESXi Unsupported Version Detection	Critical	
VMware ESXi 5.1 < Build 3021178 OpenSLP RCE (VMSA-2015-0007)	Critical	
Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities	High	
Apache 2.4.x < 2.4.39 Multiple Vulnerabilities	High	
Apache 2.4.x < 2.4.46 Multiple Vulnerabilities	High	
ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)	High	
Flexera FlexNet Publisher < 11.16.2 Multiple Vulnerabilities	High	
Microsoft Windows SMB NULL Session Authentication	High	
Microsoft Windows SMBv1 Multiple Vulnerabilities	High	
MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	High	
MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	High	
Rockwell Automation RSLinx Classic ENGINE.dll Stack Buffer Overflow	High	
Rockwell Automation RSLinx Classic ENGINE.dll Stack Buffer Overflow (CVE-2019-6553)	High	
SNMP Agent Default Community Name (public)	High	
SSL Version 2 and 3 Protocol Detection	High	
Unsupported Web Server Detection	High	
Apache 2.4.18 / 2.4.20 X.509 Certificate Authentication Bypass	Medium	

Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)	Medium	
Apache 2.4.x < 2.4.27 Multiple Vulnerabilities	Medium	
Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed)	Medium	
Apache 2.4.x < 2.4.33 Multiple Vulnerabilities	Medium	
Apache 2.4.x < 2.4.34 Multiple Vulnerabilities	Medium	
Apache 2.4.x < 2.4.35 DoS	Medium	
Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	Medium	
Apache 2.4.x < 2.4.41 Multiple Vulnerabilities	Medium	
Apache 2.4.x < 2.4.42 Multiple Vulnerabilities	Medium	
AXIS gSOAP Message Handling RCE (ACV-116267) (Devil's Ivy)	Medium	
ESXi 5.0 / 5.1 / 5.5 / 6.0 Multiple Vulnerabilities (VMSA-2016-0010) (remote check)	Medium	
ESXi 5.1 < Build 2323231 glibc Library Multiple Vulnerabilities (remote check)	Medium	
ESXi 5.1 < Build 2323236 Third-Party Libraries Multiple Vulnerabilities (remote check) (BEAST)	Medium	
ESXi 5.1 < Build 3070626 Shared Folders (HGFS) Guest Privilege Escalation (VMSA-2016-0001) (remote check)	Medium	
HSTS Missing From HTTPS Server (RFC 6797)	Medium	
HTTP TRACE / TRACK Methods Allowed	Medium	
IP Forwarding Enabled	Medium	
JQuery 1.2 < 3.5.0 Multiple XSS	Medium	
mDNS Detection (Remote Network)	Medium	
Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Medium	
MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	Medium	
OpenSSL 1.0.2 < 1.0.2k Multiple Vulnerabilities	Medium	
OpenSSL 1.0.2 < 1.0.2n Multiple Vulnerabilities	Medium	
OpenSSL 1.0.2 < 1.0.2u Procedure Overflow Vulnerability	Medium	
OpenSSL 1.0.2 < 1.0.2x Null Pointer Dereference Vulnerability	Medium	
OpenSSL 1.0.x < 1.0.2m RSA/DSA Unspecified Carry Issue	Medium	
OpenSSL 1.0.x < 1.0.2o Multiple Vulnerabilities	Medium	
OpenSSL 1.0.x < 1.0.2p Multiple Vulnerabilities	Medium	
OpenSSL 1.0.x < 1.0.2q Multiple Vulnerabilities	Medium	

OpenSSL 1.0.x < 1.0.2r Information Disclosure Vulnerability	Medium	
OpenSSL 1.1.1 < 1.1.1e-dev Procedure Overflow Vulnerability	Medium	
OpenSSL 1.1.1 < 1.1.1g Vulnerability	Medium	
OpenSSL 1.1.1 < 1.1.1i Null Pointer Dereference Vulnerability	Medium	
Rockwell Automation FactoryTalk Linx Path Traversal Information Disclosure	Medium	
SMB Signing not required	Medium	
SNMP 'GETBULK' Reflection DDoS	Medium	
SSH Weak Algorithms Supported	Medium	
SSL Certificate Cannot Be Trusted	Medium	
SSL Certificate Expiry	Medium	
SSL Certificate Signed Using Weak Hashing Algorithm	Medium	
SSL Certificate with Wrong Hostname	Medium	
SSL Medium Strength Cipher Suites Supported (SWEET32)	Medium	
SSL Self-Signed Certificate	Medium	
SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Medium	
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Medium	
Terminal Services Doesn't Use Network Level Authentication (NLA) Only	Medium	
Terminal Services Encryption Level is Medium or Low	Medium	
Unencrypted Telnet Server	Medium	
VMware ESXi Multiple DoS (VMSA-2014-0008)	Medium	
VMware ESXi Multiple Vulnerabilities (VMSA-2014-0012)	Medium	
DHCP Server Detection	Low	
OpenSSL 1.0.2 < 1.0.2t Multiple Vulnerabilities	Low	
SSH Server CBC Mode Ciphers Enabled	Low	
SSH Weak MAC Algorithms Enabled	Low	
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Low	
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Low	
Terminal Services Encryption Level is not FIPS-140 Compliant	Low	
Transport Layer Security (TLS) Protocol CRIME Vulnerability	Low	
Apache Banner Linux Distribution Disclosure	Informational	

Apple iOS Lockdown Detection	Informational	
Appweb HTTP Server Version	Informational	
AXIS FTP Server Detection	Informational	
Backported Security Patch Detection (FTP)	Informational	
Backported Security Patch Detection (PHP)	Informational	
Backported Security Patch Detection (WWW)	Informational	
Citrix Licensing Service Detection	Informational	
COM+ Internet Services (CIS) Server Detection	Informational	
DNS Server Version Detection	Informational	
Do not scan printers (AppSocket)	Informational	
Dropbox Software Detection (uncredentialed check)	Informational	
Enumerate IPv6 Interfaces via SSH	Informational	
EtherNet/IP CIP Device Identification	Informational	
FTP Server Detection	Informational	
Grandstream Phone Web Interface Detection	Informational	
LDAP Crafted Search Request Server Information Disclosure	Informational	
lighttpd HTTP Server Detection	Informational	
Link-Local Multicast Name Resolution (LLMNR) Detection	Informational	
mDNS Detection (Local Network)	Informational	
Microsoft SQL Server UDP Query Remote Version Disclosure	Informational	
Microsoft Windows SMB LanMan Pipe Server Listing Disclosure	Informational	
MongoDB Detection	Informational	
MSRPC Service Detection	Informational	
NFS Server Superfluous	Informational	
NFS Share Export List	Informational	
ONVIF Device Services	Informational	
Open Network Video Interface Forum (ONVIF) Protocol Detection	Informational	
Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	Informational	
Service Detection: 3 ASCII Digit Code Responses	Informational	
Session Initiation Protocol Detection	Informational	

Splunk Management API Detection	Informational	
Splunk Web Detection	Informational	
SSL Certificate Signed Using SHA-1 Algorithm	Informational	
SSL Cipher Block Chaining Cipher Suites Supported	Informational	
SSL Compression Methods Supported	Informational	
STUN Detection	Informational	
Target Credential Status by Authentication Protocol - No Credentials Provided	Informational	
TeamViewer remote detection	Informational	
Telnet Server Detection	Informational	
TLS Version 1.3 Protocol Detection	Informational	
Universal Plug and Play (UPnP) Protocol Detection	Informational	
VMWare STARTTLS Support	Informational	
VNC Server Unencrypted Communication Detection	Informational	
WebDAV Detection	Informational	
Web Server UPnP Detection	Informational	

Vulnerability Findings

This section of the report contains all of the vulnerabilities that were discovered for each component conducted throughout the vulnerability assessment.

Internal Network Vulnerability Assessment

Engagement Scope of Work

Through discussions with Demo Client's staff, the following target applications, IP addresses, and/or ranges were included as part of the engagement scope.

IP ADDRESSES & RANGES			
10.100.1.0/24	10.100.2.0/24	10.100.3.0/24	10.100.3.0/24
10.100.4.0/24	10.100.5.0/24	10.100.6.0/24	10.100.7.0/24
10.100.20.0/24	10.100.31.0/24	10.100.32.0/24	10.100.33.0/24
10.100.34.0/24	10.100.35.0/24	192.168.2.0/24	192.168.204.0/24

Demo Client's IT staff also provided vPenTest Partner with IP addresses and ranges to exclude. The following table displays the list of excluded systems.

EXCLUDED IP ADDRESSES & RANGES			
10.100.35.8	10.100.35.9	10.100.35.10	10.100.35.11
10.100.35.12	10.100.35.13	10.100.35.14	10.100.35.15
10.100.35.16	10.100.34.33	10.100.34.34	10.100.34.35
10.100.34.36	10.100.34.37	10.100.34.38	10.100.34.39
10.100.35.17	10.100.35.18	10.100.35.19	10.100.35.20
10.100.35.21	10.100.35.22	10.100.35.23	10.100.35.24
10.100.35.25	10.100.35.26	10.100.35.27	10.100.35.28
10.100.35.29	10.100.35.30	10.100.35.31	10.100.35.32
10.100.35.33	10.100.35.34	10.100.35.35	10.100.35.36
10.100.35.37	10.100.35.38	10.100.35.39	10.100.35.40
10.100.35.41	10.100.35.42	10.100.35.43	10.100.35.44
10.100.35.45	10.100.35.46	10.100.35.47	10.100.35.48
10.100.35.49	10.100.35.50		

AXIS HTTP GET Heap Overflow	
Severity	
Description	The remote AXIS device is affected by a heap overflow vulnerability in its web administration interface due to a flaw in handling of special characters. An unauthenticated remote attacker can exploit this vulnerability for denial of service and possibly remote code execution. The remote device is affected by an heap overflow vulnerability that may lead to remote code execution.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	9.3 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Recommendation	Follow the vendor recommendation for upgrade or mitigation.
References	https://www.axis.com/files/faq/Advisory_ACV-120444.pdf
Affected Nodes	10.100.7.150 on port 80/tcp 10.100.6.87 on port 80/tcp 10.100.3.151 on port 80/tcp

Additional Output	`The following URL can be used to trigger a heap overflow:`
	
	`http://10.100.7.150/index.shtml`

AXIS Multiple Vulnerabilities (ACV-128401)	
Severity	
Description	The firmware version running on the remote host is vulnerable to multiple vulnerabilities. An unauthenticated remote attacker could gain system-level unauthorized access to the affected device. Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote host is affected by multiple vulnerabilities.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade the host firmware to the version provided in the affected product list.
References	http://www.nessus.org/u?471d8c96 https://www.axis.com/files/faq/Advisory_ACV-128401.pdf https://www.axis.com/files/sales/ACV-128401_Affected_Product_List.pdf
Affected Nodes	10.100.33.20 on port 80/tcp 10.100.6.87 on port 80/tcp 10.100.3.151 on port 21/tcp 10.100.3.150 on port 21/tcp 10.100.1.151 on port 443/tcp 10.100.1.150 on port 443/tcp
Additional Output	`Installed version : 7.30.1` `  Fixed version     : 8.20.1`

Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	
Severity	
Description	The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Recommendation	Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.
References	n/a
Affected Nodes	10.100.7.210 on port 3389/tcp 10.100.7.131 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.115 on port 3389/tcp 10.100.7.136 on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp
Additional Output	n/a

Microsoft SQL Server Unsupported Version Detection (remote check)

Severity	
Description	According to its self-reported version number, the installation of Microsoft SQL Server on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. An unsupported version of a database server is running on the remote host.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Recommendation	Upgrade to a version of Microsoft SQL Server that is currently supported.
References	http://www.nessus.org/u?d4418a57
Affected Nodes	192.168.2.18 on port 54433/tcp 10.100.20.200 on port 1433/tcp 10.100.7.119 on port 1433/tcp 10.100.7.116 on port 1433/tcp 10.100.7.53 (URSHISTSVR01) on port 1433/tcp 10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp 10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp
Additional Output	The following unsupported installation of Microsoft SQL Server was detected : Installed version : 12.0.4237.0 Fixed version : 12.0.5000.0 (2014 SP2) SQL Server Instance : SWPDM

Microsoft Windows XP Unsupported Installation Detection

Severity	
Description	The remote host is running Microsoft Windows XP. Support for this operating system by Microsoft ended April 8th, 2014. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Recommendation	Upgrade to a version of Windows that is currently supported.
References	n/a
Affected Nodes	10.100.7.136 on port 0/tcp
Additional Output	

	n/a

MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	
Severity	
Description	The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the Secure Channel (Schannel) security package. An attacker can exploit this issue by sending specially crafted packets to a Windows server. Note that this plugin sends a client Certificate TLS handshake message followed by a CertificateVerify message. Some Windows hosts will close the connection upon receiving a client certificate for which it did not ask for with a CertificateRequest message. In this case, the plugin cannot proceed to detect the vulnerability as the CertificateVerify message cannot be sent.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	8.8 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2.
References	n/a
Affected Nodes	10.100.7.115 on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp
Additional Output	n/a

Unix Operating System Unsupported Version Detection	
Severity	
Description	According to its self-reported version number, the Unix operating system running on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. The operating system running on the remote host is no longer supported.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Recommendation	Upgrade to a version of the Unix operating system that is currently supported.
References	n/a
Affected Nodes	192.168.2.5 on port 0/tcp 192.168.2.3 on port 0/tcp
Additional Output	VMware ESXi 5. support ended on 2018-09-19. Upgrade to VMware ESXi 6.7.0 build-10764712. For more information, see : https://docs.vmware.com/en/VMware-vSphere/

Unsupported Windows OS (remote)	
Severity	
Description	The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities. The remote OS or service pack is no longer supported.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade to a supported service pack or operating system

References	https://support.microsoft.com/en-us/lifecycle
Affected Nodes	10.100.7.210 on port 0/tcp 10.100.7.136 on port 0/tcp 10.100.7.135 on port 0/tcp 10.100.7.131 on port 0/tcp 10.100.7.125 on port 0/tcp 10.100.7.111 on port 0/tcp 10.100.7.115 on port 0/tcp 10.100.5.64 (CONMSAUTHMI601) on port 0/tcp 10.100.5.59 (IT06-G8F8HF1) on port 0/tcp

Additional Output	`The following Windows version is installed and not supported:`
	
	`Microsoft Windows 7 Professional`

VMware ESX / ESXi Unsupported Version Detection

Severity	
Description	According to its version, the installation of VMware ESX or ESXi on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. The remote host is running an unsupported version of a virtualization application.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Recommendation	Upgrade to a version of VMware ESX / ESXi that is currently supported.
References	https://www.vmware.com/support/policies/lifecycle.html https://www.vmware.com/files/pdf/support/Product-Lifecycle-Matrix.pdf
Affected Nodes	192.168.2.5 on port 0/tcp 192.168.2.3 on port 0/tcp

Additional Output	`Product : ESXi`
	`Installed version : 5.1`
	`EOL date : August 08, 2016`
	`Supported versions : 6.5 / 6.7 / 7.0`

VMware ESXi 5.1 < Build 3021178 OpenSLP RCE (VMSA-2015-0007)

Severity	
Description	The remote VMware ESXi host is version 5.1 prior to build 3021178. It is, therefore, affected by a remote code execution vulnerability due to a double-free error in the SLPDProcessMessage() function in OpenSLP. An unauthenticated, remote attacker can exploit this, via a crafted package, to execute arbitrary code or cause a denial of service condition. The remote VMware ESXi host is affected by a remote code execution vulnerability.
CVSS	10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	8.6 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H)
Recommendation	Apply patch ESXi510-201510101-SG for ESXi 5.1.
References	https://www.vmware.com/security/advisories/VMSA-2015-0007.html https://www.zerodayinitiative.com/advisories/ZDI-15-455/
Affected Nodes	192.168.2.5 on port 0/tcp 192.168.2.3 on port 0/tcp

Additional Output	`ESXi version : ESXi 5.1`
	`Installed build : 2000251`
	`Fixed build : 3021178`

Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities	
Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.2.x prior to 2.2.33-dev or 2.4.x prior to 2.4.26. It is, therefore, affected by the following vulnerabilities : - An authentication bypass vulnerability exists due to third-party modules using the ap_get_basic_auth_pw() function outside of the authentication phase. An unauthenticated, remote attacker can exploit this to bypass authentication requirements. (CVE-2017-3167) - A NULL pointer dereference flaw exists due to third-party module calls to the mod_ssl ap_hook_process_connection() function during an HTTP request to an HTTPS port. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (CVE-2017-3169) - A NULL pointer dereference flaw exists in mod_http2 that is triggered when handling a specially crafted HTTP/2 request. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. Note that this vulnerability does not affect 2.2.x. (CVE-2017-7659) - An out-of-bounds read error exists in the ap_find_token() function due to improper handling of header sequences. An unauthenticated, remote attacker can exploit this, via a specially crafted header sequence, to cause a denial of service condition. (CVE-2017-7668) - An out-of-bounds read error exists in mod_mime due to improper handling of Content-Type response headers. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type response header, to cause a denial of service condition or the disclosure of sensitive information. (CVE-2017-7679) Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade to Apache version 2.2.33-dev / 2.4.26 or later.
References	https://archive.apache.org/dist/httpd/CHANGES_2.2.32 https://archive.apache.org/dist/httpd/CHANGES_2.4.26 https://httpd.apache.org/security/vulnerabilities_22.html https://httpd.apache.org/security/vulnerabilities_24.html
Affected Nodes	10.100.6.87 on port 80/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.26`

Apache 2.4.x < 2.4.39 Multiple Vulnerabilities	
Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.39. It is, therefore, affected by multiple vulnerabilities: - A privilege escalation vulnerability exists in module scripts due to an ability to execute arbitrary code as the parent process by manipulating the scoreboard. (CVE-2019-0211) - An access control bypass vulnerability exists in mod_auth_digest due to a race condition when running in a threaded server. An attacker with valid credentials could authenticate using another username. (CVE-2019-0217) - An access control bypass vulnerability exists in mod_ssl when using per-location client certificate verification with TLSv1.3. (CVE-2019-0215) In addition, Apache httpd is also affected by several additional vulnerabilities including a denial of service, read-

	after-free and URL path normalization inconsistencies. Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade to Apache version 2.4.39 or later.
References	http://www.nessus.org/u?a84bee48 http://www.nessus.org/u?586e6a34
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 443/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.39`

Apache 2.4.x < 2.4.46 Multiple Vulnerabilities

Severity	
Description	The version of Apache httpd installed on the remote host is prior to 2.4.44. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.46 advisory. - Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE (CVE-2020-11984) - Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above info will mitigate this vulnerability for unpatched servers. (CVE-2020-11993) - Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via H2Push off will mitigate this vulnerability for unpatched servers. (CVE-2020-9490) Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade to Apache version 2.4.44 or later.
References	n/a
Affected Nodes	10.100.31.82 on port 80/tcp 10.100.31.82 on port 80/tcp 10.100.31.82 on port 80/tcp 10.100.31.82 on port 443/tcp 10.100.31.82 on port 443/tcp 10.100.31.81 on port 80/tcp 10.100.31.81 on port 80/tcp 10.100.31.81 on port 80/tcp 10.100.31.81 on port 443/tcp 10.100.31.81 on port 443/tcp 10.100.31.81 on port 443/tcp 10.100.31.69 on port 80/tcp 10.100.31.69 on port 80/tcp

	10.100.31.69 on port 443/tcp 10.100.31.69 on port 443/tcp 10.100.31.60 on port 80/tcp 10.100.31.60 on port 80/tcp 10.100.31.60 on port 443/tcp 10.100.31.82 on port 443/tcp 10.100.31.69 on port 80/tcp 10.100.31.69 on port 443/tcp 10.100.31.60 on port 80/tcp 10.100.31.60 on port 443/tcp 10.100.31.60 on port 443/tcp 10.100.31.54 on port 80/tcp 10.100.31.54 on port 80/tcp 10.100.31.54 on port 80/tcp 10.100.31.54 on port 443/tcp 10.100.31.54 on port 443/tcp 10.100.31.54 on port 443/tcp 10.100.31.52 on port 80/tcp 10.100.31.52 on port 80/tcp 10.100.31.52 on port 80/tcp 10.100.31.52 on port 443/tcp 10.100.31.52 on port 443/tcp 10.100.31.52 on port 443/tcp 10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 443/tcp

Additional Output	`URL : http://10.100.31.82/`
	`Installed version : 2.4.41`
	`Fixed version : 2.4.46`

ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)	
Severity	
Description	According to its self-reported version number, the remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by multiple vulnerabilities. - A use-after-free error exists in the XHCI USB controller. An unauthenticated, local attacker with local administrative privileges on a virtual machine can exploit this, to execute code as the virtual machine's VMX process running on the host. (CVE-2020-4004) - A privilege escalation vulnerability exists in ESXi due to how certain system calls are managed. An authenticated, local attacker with privileges within the VPM process can exploit this, when chained with CVE-2020-4004, to obtain escalated privileges. (CVE-2020-4005) Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote VMware ESXi host is missing a security patch and is affected by multiple vulnerabilities.
CVSS	7.2 (CVSS2#AV:L/AC:L/Au:N/C:C/I:C/A:C)
CVSS3	7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Apply the appropriate patch as referenced in the vendor advisory.
References	https://www.vmware.com/security/advisories/VMSA-2020-0026.html
Affected Nodes	10.100.7.96 on port 443/tcp 10.100.7.95 (IT09-5Z5KN53) on port 443/tcp 10.100.2.60 on port 443/tcp 10.100.2.58 on port 443/tcp 10.100.2.57 on port 443/tcp 10.100.2.56 on port 443/tcp
Additional Output	`ESXi version : 7.0` `Installed build : 16324942`

	Fixed build : 17168206

Flexera FlexNet Publisher < 11.16.2 Multiple Vulnerabilities	
Severity	
Description	The version of Flexera FlexNet Publisher running on the remote host is prior to 11.16.2. It is, therefore, affected by multiple vulnerabilities : - A Denial of Service vulnerability related to preemptive item deletion in lmgrd and vendor daemon components of FlexNet Publisher version 11.16.1.0 and earlier allows a remote attacker to send a combination of messages to lmgrd or the vendor daemon, causing the heartbeat between lmgrd and the vendor daemon to stop, and the vendor daemon to shut down. (CVE-2018-20031) - A Denial of Service vulnerability related to message decoding in lmgrd and vendor daemon components of FlexNet Publisher version 11.16.1.0 and earlier allows a remote attacker to send a combination of messages to lmgrd or the vendor daemon, causing the heartbeat between lmgrd and the vendor daemon to stop, and the vendor daemon to shut down. (CVE-2018-20032) - A Remote Code Execution vulnerability in lmgrd and vendor daemon components of FlexNet Publisher version 11.16.1.0 and earlier could allow a remote attacker to corrupt the memory by allocating / deallocating memory, loading lmgrd or the vendor daemon and causing the heartbeat between lmgrd and the vendor daemon to stop. This would force the vendor daemon to shut down. (CVE-2018-20033) - A Denial of Service vulnerability related to adding an item to a list in lmgrd and vendor daemon components of FlexNet Publisher version 11.16.1.0 and earlier allows a remote attacker to send a combination of messages to lmgrd or the vendor daemon, causing the heartbeat between lmgrd and the vendor daemon to stop, and the vendor daemon to shut down. (CVE-2018-20034) A licensing application running on the remote host is affected by multiple vulnerabilities.
CVSS	7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade to FlexNet Publisher 11.16.2 or later.
References	http://www.nessus.org/u?eb4f204b http://www.nessus.org/u?fbd5ba7b
Affected Nodes	192.168.2.18 on port 27000/tcp 10.100.20.200 on port 27000/tcp 10.100.7.110 on port 27000/tcp 10.100.7.93 (OWS-01A) on port 27000/tcp 10.100.7.90 (HMI-01B) on port 27000/tcp 10.100.7.86 (HIST-01A) on port 27000/tcp 10.100.7.77 (HMI-01A) on port 27000/tcp 10.100.7.70 (EWS-01) on port 27000/tcp 10.100.5.68 (IT02-2SD5Y2) on port 27000/tcp 10.100.3.64 (IT01-4P775Y2) on port 27000/tcp 10.100.2.49 (IT09-H42HYV1) on port 27000/tcp
Additional Output	`Installed version : 11.12.1` `  Fixed version : 11.16.2`

Microsoft Windows SMB NULL Session Authentication	
Severity	
Description	The remote host is running Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password). Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host. It is possible to log into the remote Windows host with a NULL session.

CVSS	7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS3	7.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)
Recommendation	Apply the following registry changes per the referenced Technet advisories : Set : - HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1 - HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1 Reboot once the registry changes are complete.
References	http://www.nessus.org/u?5c2589f6 http://www.nessus.org/u?899b4072 http://www.nessus.org/u?a33fe205
Affected Nodes	10.100.7.136 on port 445/tcp
Additional Output	`It was possible to bind to the \browser pipe`

Microsoft Windows SMBv1 Multiple Vulnerabilities

Severity	
Description	The remote Windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled. It is, therefore, affected by multiple vulnerabilities : - Multiple information disclosure vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to disclose sensitive information. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276) - Multiple denial of service vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMB request, to cause the system to stop responding. (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280) - Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to execute arbitrary code. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279) Depending on the host's security policy configuration, this plugin cannot always correctly determine if the Windows host is vulnerable if the host is running a later Windows version (i.e., Windows 8.1, 10, 2012, 2012 R2, and 2016) specifically that named pipes and shares are allowed to be accessed remotely and anonymously. Tenable does not recommend this configuration, and the hosts should be checked locally for patches with one of the following plugins, depending on the Windows version : 100054, 100055, 100057, 100059, 100060, or 100061.
CVSS	9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)
CVSS3	8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Apply the applicable security update for your Windows version : - Windows Server 2008 : KB4018466 - Windows 7 : KB4019264 - Windows Server 2008 R2 : KB4019264 - Windows Server 2012 : KB4019216 - Windows 8.1 / RT 8.1. : KB4019215 - Windows Server 2012 R2 : KB4019215 - Windows 10 : KB4019474 - Windows 10 Version 1511 : KB4019473 - Windows 10 Version 1607 : KB4019472 - Windows 10 Version 1703 : KB4016871 - Windows Server 2016 : KB4019472
References	n/a
Affected Nodes	10.100.7.136 on port 445/tcp 10.100.7.131 on port 445/tcp 10.100.7.115 on port 445/tcp
Additional Output	`n/a`

MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	
Severity	
Description	An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted. If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it. This plugin also checks for a denial of service vulnerability in Microsoft Terminal Server. Note that this script does not detect the vulnerability if the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting is enabled or the security layer is set to 'SSL (TLS 1.0)' on the remote host.
CVSS	9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)
Recommendation	Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2. Note that an extended support contract with Microsoft is required to obtain the patch for this vulnerability for Windows 2000.
References	n/a
Affected Nodes	10.100.7.136 on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp
Additional Output	n/a

MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	
Severity	
Description	The remote Windows host is affected by the following vulnerabilities : - Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) - An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147) ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.
CVSS	9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)
CVSS3	8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8. For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.
References	n/a

Affected Nodes	10.100.7.131 on port 445/tcp 10.100.7.136 on port 445/tcp 10.100.7.115 on port 445/tcp 10.100.5.64 (CONMSAUTHMI601) on port 445/tcp
Additional Output	Sent: 00000054ff534d4225000000001803c800000000000000000000000006105b660180000110000000 00ffffffff0000000000000000000000540000005400020023000001100005c00500049005000 45005c0000000000 Received: ff534d4225050200c09803c8000000000000000000000000006105b6601800001000000

Rockwell Automation RSLinx Classic ENGINE.dll Stack Buffer Overflow	
Severity	
Description	The RSLinx Classic running on the remote host is affected by a remote code execution vulnerability due to a stack buffer overflow condition when handling an EtherNet/IP message received on TCP port 44818. An unauthenticated, remote attacker can exploit this issue, via a specially crafted message, to execute arbitrary code. Note that RSLinx Classic is reportedly affected by additional vulnerabilities; however, this plugin has not tested for these.
CVSS	7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Patches are available for versions 4.00.01, 3.90.01, 3.81, 3.80, 3.74, and 3.60. See vendor Knowledgebase Article ID 1075712 for more details.
References	n/a
Affected Nodes	10.100.7.125 on port 44818/tcp
Additional Output	n/a

Rockwell Automation RSLinx Classic ENGINE.dll Stack Buffer Overflow (CVE-2019-6553)	
Severity	
Description	The RSLinx Classic running on the remote host is affected by a remote code execution vulnerability due to a stack buffer overflow condition when handling an EtherNet/IP message received on TCP port 44818. An unauthenticated, remote attacker can exploit this issue, via a specially crafted message, to execute arbitrary code.
CVSS	7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Patches are available for versions 4.10, 4.00.01, 3.90, 3.81, 3.80, 3.70, and 3.60. See vendor Knowledgebase Article ID 1085038 for more details.
References	n/a
Affected Nodes	10.100.7.125 on port 44818/tcp
Additional Output	n/a

SNMP Agent Default Community Name (public)	
Severity	
Description	It is possible to obtain the default community name of the remote SNMP server. An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications). The community name of the remote SNMP server can be guessed.

CVSS	7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
Recommendation	Disable the SNMP service on the remote host if you do not use it. Either filter incoming UDP packets going to this port, or change the default community string.
References	n/a
Affected Nodes	192.168.2.58 on port 161/udp 192.168.2.57 on port 161/udp 192.168.2.56 on port 161/udp 192.168.2.55 on port 161/udp 192.168.2.46 on port 161/udp 192.168.2.28 on port 161/udp 192.168.2.16 on port 161/udp 192.168.2.14 on port 161/udp 192.168.2.13 on port 161/udp 192.168.2.7 on port 161/udp 192.168.2.4 on port 161/udp 192.168.2.2 on port 161/udp 192.168.2.20 on port 161/udp 10.100.7.68 on port 161/udp 10.100.7.67 on port 161/udp 10.100.7.64 on port 161/udp 10.100.7.63 on port 161/udp 10.100.6.26 on port 161/udp 10.100.6.25 on port 161/udp 10.100.3.63 on port 161/udp 10.100.1.35 on port 161/udp

Additional Output	`The remote SNMP server replies to the following default community string :`
	
	`public`

SSL Version 2 and 3 Protocol Detection

Severity	
Description	The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients. Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely. NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'. The remote service encrypts traffic using a protocol with known weaknesses.
CVSS	7.1 (CVSS2#AV:N/AC:M/Au:N/C:C/I:N/A:N)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.1 (with approved cipher suites) or higher instead.
References	https://www.schneier.com/academic/paperfiles/paper-ssl.pdf http://www.nessus.org/u?b06c7e95 http://www.nessus.org/u?247c4540 https://www.openssl.org/~bodo/ssl-poodle.pdf

	http://www.nessus.org/u?5d15ba70 https://www.imperialviolet.org/2014/10/14/poodle.html https://tools.ietf.org/html/rfc7507 https://tools.ietf.org/html/rfc7568
Affected Nodes	192.168.2.63 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.59 on port 443/tcp 192.168.2.51 on port 443/tcp 192.168.2.64 on port 443/tcp 192.168.2.61 on port 443/tcp 192.168.2.18 on port 54433/tcp 192.168.2.19 on port 443/tcp 192.168.2.5 on port 902/tcp 192.168.2.5 on port 5989/tcp 192.168.2.5 on port 443/tcp 192.168.2.3 on port 902/tcp 192.168.2.3 on port 5989/tcp 192.168.2.3 on port 443/tcp 10.100.7.210 on port 3071/tcp 10.100.7.116 on port 1433/tcp 10.100.7.111 on port 3071/tcp 10.100.20.200 on port 1433/tcp 10.100.7.119 on port 1433/tcp 10.100.7.53 (URSHISTSVR01) on port 1433/tcp 10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp 10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp
Additional Output	- SSLv3 is enabled and the server supports at least one cipher. Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3 Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES) Name Code KEX Auth Encryption MAC DES-CBC3-SHA RSA RSA 3DES-CBC(168) SHA1 High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC AES256-SHA RSA RSA AES-CBC(256) SHA1 RC4-SHA RSA RSA RC4(128) SHA1 The fields above are : {Tenable ciphernam ------------ snipped ------------

Unsupported Web Server Detection	
Severity	
Description	According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities. The remote web server is obsolete / unsupported.
CVSS	7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS3	10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Recommendation	Remove the service if it is no longer needed. Otherwise, upgrade to a newer version if possible or switch to another server.
References	n/a
Affected Nodes	10.100.5.64 (CONMSAUTHMI601) on port 80/tcp

Additional Output	Product : Microsoft IIS 7.5 Server response header : Microsoft-IIS/7.5 Support ended : 2020-01-14 Supported versions : Microsoft IIS 8.5 / 8.0 Additional information : http://www.nessus.org/u?a4f4b8ab

Apache 2.4.18 / 2.4.20 X.509 Certificate Authentication Bypass

Severity	
Description	According to its banner, the version of Apache running on the remote host is either 2.4.18 or 2.4.20. Additionally, HTTP/2 is enabled over TLS or SSL. It is, therefore, affected by the an authentication bypass vulnerability in the experimental module for the HTTP/2 protocol due to a failure to correctly validate X.509 certificates, allowing access to resources that otherwise would not be allowed. An unauthenticated, remote attacker can exploit this to disclose potentially sensitive information. The remote web server is affected by an authentication bypass vulnerability.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
Recommendation	Upgrade to Apache version 2.4.23 or later. Alternatively, as a temporary workaround, HTTP/2 can be disabled by changing the configuration by removing 'h2' and 'h2c' from the Protocols line(s) in the configuration file.
References	https://archive.apache.org/dist/httpd/CHANGES_2.4.23 https://httpd.apache.org/security/vulnerabilities_24.html https://seclists.org/fulldisclosure/2016/Jul/11
Affected Nodes	10.100.6.87 on port 80/tcp
Additional Output	URL : http://10.100.6.87/ Installed version : 2.4.20 Fixed version : 2.4.23

Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)

Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.25. It is, therefore, affected by the following vulnerabilities : - A flaw exists in the mod_session_crypto module due to encryption for data and cookies using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default). An unauthenticated, remote attacker can exploit this, via a padding oracle attack, to decrypt information without knowledge of the encryption key, resulting in the disclosure of potentially sensitive information. (CVE-2016-0736) - A denial of service vulnerability exists in the mod_auth_digest module during client entry allocation. An unauthenticated, remote attacker can exploit this, via specially crafted input, to exhaust shared memory resources, resulting in a server crash. (CVE-2016-2161) - The Apache HTTP Server is affected by a man-in-the-middle vulnerability known as 'httpoxy' due to a failure to properly resolve namespace conflicts in accordance with RFC 3875 section 4.1.18. The HTTP_PROXY environment variable is set based on untrusted user data in the 'Proxy' header of HTTP requests. The HTTP_PROXY environment variable is used by some web client libraries to specify a remote proxy server. An unauthenticated, remote attacker can exploit this, via a crafted 'Proxy' header in an HTTP request, to redirect an application's internal HTTP traffic to an arbitrary proxy server where it may be observed or manipulated. (CVE-2016-5387) - A denial of service vulnerability exists in the mod_http2 module due to improper handling of the LimitRequestFields directive. An unauthenticated, remote attacker can exploit this, via specially crafted CONTINUATION frames in an HTTP/2 request, to inject unlimited request headers into the server, resulting in the exhaustion of memory resources. (CVE-2016-8740) - A flaw exists due to improper handling of whitespace patterns in user-agent headers. An unauthenticated, remote attacker can exploit this, via a specially crafted user-agent header, to cause the program to incorrectly process sequences of requests, resulting in interpreting responses incorrectly, polluting the cache, or disclosing the content from one request to a second downstream user-agent. (CVE-2016-8743)

	- A CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir (CVE-2016-4975) Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)
CVSS3	8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade to Apache version 2.4.25 or later. Note that the 'httpoxy' vulnerability can be mitigated by applying the workarounds or patches as referenced in the vendor advisory asf-httpoxy-response.txt. Furthermore, to mitigate the other vulnerabilities, ensure that the affected modules (mod_session_crypto, mod_auth_digest, and mod_http2) are not in use.
References	https://httpd.apache.org/dev/dist/Announcement2.4.html http://httpd.apache.org/security/vulnerabilities_24.html https://github.com/apache/httpd/blob/2.4.x/CHANGES https://www.apache.org/security/asf-httpoxy-response.txt https://httpoxy.org
Affected Nodes	10.100.6.87 on port 80/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.25`

Apache 2.4.x < 2.4.27 Multiple Vulnerabilities

Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.27. It is, therefore, affected by the following vulnerabilities : - A denial of service vulnerability exists in httpd due to a failure to initialize or reset the value placeholder in [Proxy-]Authorization headers of type 'Digest' before or between successive key=value assignments by mod_auth_digest. An unauthenticated, remote attacker can exploit this, by providing an initial key with no '=' assignment, to disclose sensitive information or cause a denial of service condition. (CVE-2017-9788) - A read-after-free error exists in httpd that is triggered when closing a large number of connections. An unauthenticated, remote attacker can exploit this to have an unspecified impact. (CVE-2017-9789) Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:P)
CVSS3	9.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H)
Recommendation	Upgrade to Apache version 2.4.27 or later.
References	https://archive.apache.org/dist/httpd/CHANGES_2.4.27 https://httpd.apache.org/security/vulnerabilities_24.html
Affected Nodes	10.100.6.87 on port 80/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.27`

Apache 2.4.x < 2.4.28 HTTP Vulnerability (OptionsBleed)

Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.28. It is, therefore,

	affected by an HTTP vulnerability related to the directive in an .htaccess file. Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Upgrade to Apache version 2.4.28 or later.
References	https://archive.apache.org/dist/httpd/CHANGES_2.4.28 https://httpd.apache.org/security/vulnerabilities_24.html
Affected Nodes	10.100.6.87 on port 80/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.28`

Apache 2.4.x < 2.4.33 Multiple Vulnerabilities

Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.33. It is, therefore, affected by multiple vulnerabilities: - An out of bounds write vulnerability exists in mod_authnz_ldap with AuthLDAPCharsetConfig enabled. An unauthenticated, remote attacker can exploit this, via the Accept-Language header value, to cause the application to stop responding. (CVE-2017-15710) - An arbitrary file upload vulnerability exists in the FilesMatch component where a malicious filename can be crafted to match the expression check for a newline character. An unauthenticated, remote attacker can exploit this, via newline character, to upload arbitrary files on the remote host subject to the privileges of the user. (CVE-2017-15715) - A session management vulnerability exists in the mod_session component due to SessionEnv being enabled and forwarding it's session data to the CGI Application. An unauthenticated, remote attacker can exploit this, via tampering the HTTP_SESSION and using a session header, to influence content. (CVE-2018-1283) - An out of bounds access vulnerability exists when the size limit is reached. An unauthenticated, remote attacker can exploit this, to cause the Apache HTTP Server to crash. (CVE-2018-1301) - A write after free vulnerability exists in HTTP/2 stream due to a NULL pointer being written to an area of freed memory. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2018-1302) - An out of bounds read vulnerability exists in mod_cache_socache. An unauthenticated, remote attacker can exploit this, via a specially crafted HTTP request header to cause the application to stop responding. (CVE-2018-1303) - A weak digest vulnerability exists in the HTTP digest authentication challenge. An unauthenticated, remote attacker can exploit this in a cluster of servers configured to use a common digest authentication, to replay HTTP requests across servers without being detected. (CVE-2018-1312) Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVSS3	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade to Apache version 2.4.33 or later.
References	https://archive.apache.org/dist/httpd/CHANGES_2.4.33 https://httpd.apache.org/security/vulnerabilities_24.html#2.4.33
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp

	10.100.6.20 on port 443/tcp 10.100.6.20 on port 80/tcp
Additional Output	URL : http://10.100.6.87/ Installed version : 2.4.20 Fixed version : 2.4.33

Apache 2.4.x < 2.4.34 Multiple Vulnerabilities	
Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.34. It is, therefore, affected by the following vulnerabilities: - By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. (CVE-2018-1333) - By specially crafting HTTP requests, the mod_md challenge handler would dereference a NULL pointer and cause the child process to segfault. This could be used to DoS the server. (CVE-2018-8011) Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
Recommendation	Upgrade to Apache version 2.4.34 or later.
References	https://archive.apache.org/dist/httpd/CHANGES_2.4.34 https://httpd.apache.org/security/vulnerabilities_24.html#2.4.34
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 443/tcp
Additional Output	URL : http://10.100.6.87/ Installed version : 2.4.20 Fixed version : 2.4.34

Apache 2.4.x < 2.4.35 DoS	
Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.35. It is, therefore, affected by the following vulnerability: - By sending continuous SETTINGS frames of maximum size an ongoing HTTP/2 connection could be kept busy and would never time out. This can be abused for a DoS on the server. This only affect a server that has enabled the h2 protocol. Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by a denial of service vulnerability.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)
CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
Recommendation	Upgrade to Apache version 2.4.35 or later.
References	https://archive.apache.org/dist/httpd/CHANGES_2.4.35 https://httpd.apache.org/security/vulnerabilities_24.html#2.4.35
Affected Nodes	10.100.6.87 on port 80/tcp

	10.100.6.20 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 443/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.35`

Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	
Severity	
Description	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.38. It is, therefore, affected by multiple vulnerabilities: - A denial of service (DoS) vulnerability exists in HTTP/2 steam handling. An unauthenticated, remote attacker can exploit this issue, via sending request bodies in a slow loris way to plain resources, to occupy a server thread. (CVE-2018-17189) - A vulnerability exists in mod_sesion_cookie, as it does not properly check the expiry time of cookies. (CVE-2018-17199) - A denial of service (DoS) vulnerability exists in mod_ssl when used with OpenSSL 1.1.1 due to an interaction in changes to handling of renegotiation attempts. An unauthenticated, remote attacker can exploit this issue to cause mod_ssl to stop responding. (CVE-2019-0190) Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
Recommendation	Upgrade to Apache version 2.4.38 or later.
References	https://archive.apache.org/dist/httpd/CHANGES_2.4.38 https://httpd.apache.org/security/vulnerabilities_24.html#2.4.38
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 443/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.38`

Apache 2.4.x < 2.4.41 Multiple Vulnerabilities	
Severity	
Description	The version of Apache httpd installed on the remote host is prior to 2.4.41. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.41 advisory. - HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with H2PushResource, could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client. (CVE-2019-10081) - Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both. (CVE-2019-9517)

	Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:P)
CVSS3	9.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H)
Recommendation	Upgrade to Apache version 2.4.41 or later.
References	n/a
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 443/tcp

Additional Output	`URL : http://10.100.6.87/`
	`Installed version : 2.4.20`
	`Fixed version : 2.4.41`

Apache 2.4.x < 2.4.42 Multiple Vulnerabilities

Severity	
Description	The version of Apache httpd installed on the remote host is prior to 2.4.42. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.42 advisory. - In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server. (CVE-2020-1934) - In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL. (CVE-2020-1927) Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote web server is affected by multiple vulnerabilities.
CVSS	5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)
CVSS3	6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
Recommendation	Upgrade to Apache version 2.4.42 or later.
References	n/a
Affected Nodes	10.100.31.82 on port 80/tcp 10.100.31.82 on port 80/tcp 10.100.31.82 on port 80/tcp 10.100.31.82 on port 443/tcp 10.100.31.82 on port 443/tcp 10.100.31.82 on port 443/tcp 10.100.31.81 on port 80/tcp 10.100.31.81 on port 80/tcp 10.100.31.81 on port 443/tcp 10.100.31.81 on port 443/tcp 10.100.31.81 on port 443/tcp 10.100.31.69 on port 80/tcp 10.100.31.69 on port 80/tcp 10.100.31.69 on port 80/tcp 10.100.31.69 on port 443/tcp 10.100.31.69 on port 443/tcp 10.100.31.69 on port 443/tcp 10.100.31.81 on port 80/tcp 10.100.31.60 on port 80/tcp 10.100.31.60 on port 80/tcp

	10.100.31.60 on port 80/tcp 10.100.31.60 on port 443/tcp 10.100.31.60 on port 443/tcp 10.100.31.60 on port 443/tcp 10.100.31.54 on port 80/tcp 10.100.31.54 on port 80/tcp 10.100.31.54 on port 80/tcp 10.100.31.54 on port 443/tcp 10.100.31.54 on port 443/tcp 10.100.31.54 on port 443/tcp 10.100.31.52 on port 80/tcp 10.100.31.52 on port 80/tcp 10.100.31.52 on port 80/tcp 10.100.31.52 on port 443/tcp 10.100.31.52 on port 443/tcp 10.100.31.52 on port 443/tcp 10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 443/tcp

Additional Output	`URL : http://10.100.31.82/`
	`Installed version : 2.4.41`
	`Fixed version : 2.4.42`

AXIS gSOAP Message Handling RCE (ACV-116267) (Devil's Ivy)

Severity	
Description	The remote AXIS device is running a firmware version that is missing a security patch. It is, therefore, affected by a remote code execution vulnerability, known as Devil's Ivy, due to an overflow condition that exists in a third party SOAP library (gSOAP). An unauthenticated, remote attacker can exploit this, via an HTTP POST message exceeding 2GB of data, to trigger a stack-based buffer overflow, resulting in a denial of service condition or the execution of arbitrary code. An attacker who successfully exploits this vulnerability can reset the device to its factory defaults, change network settings, take complete control of the device, or reboot it to prevent an operator from viewing the feed. The remote device is affected by a remote code execution vulnerability.
CVSS	6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVSS3	8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
Recommendation	Upgrade to the latest available firmware version for your device per the vendor advisory (ACV-116267).
References	https://www.axis.com/files/faq/ACV116267_(CVE-2017-9765).pdf https://www.axis.com/ftp/pub_soft/MPQT/SR/acv_116267_patched_fw.txt http://blog.senr.io/devilsivy.html
Affected Nodes	10.100.7.150 on port 0/tcp 10.100.3.150 on port 0/tcp

Additional Output	`Model : P5624-E Mk II`
	`Software version : 6.35.1.1`
	`Version source : HTTP`
	`Fixed version : 6.50.1.2`

ESXi 5.0 / 5.1 / 5.5 / 6.0 Multiple Vulnerabilities (VMSA-2016-0010) (remote check)

Severity	
Description	The remote VMware ESXi host is version 5.0, 5.1, 5.5, or 6.0 and is missing a security patch. It is, therefore, affected by multiple vulnerabilities : - An arbitrary code execution vulnerability exists in the Shared Folders (HGFS) feature due to improper loading of Dynamic-link library (DLL) files from insecure paths, including the current working directory, which may not be under

	user control. A remote attacker can exploit this vulnerability, by placing a malicious DLL in the path or by convincing a user into opening a file on a network share, to inject and execute arbitrary code in the context of the current user. (CVE-2016-5330) - An HTTP header injection vulnerability exists due to improper sanitization of user-supplied input. A remote attacker can exploit this to inject arbitrary HTTP headers and conduct HTTP response splitting attacks. (CVE-2016-5331) The remote VMware ESXi host is affected by multiple vulnerabilities.
CVSS	4.4 (CVSS2#AV:L/AC:M/Au:N/C:P/I:P/A:P)
CVSS3	7.8 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
Recommendation	Apply the appropriate patch as referenced in the vendor advisory. Note that VMware Tools on Windows-based guests that use the Shared Folders (HGFS) feature must also be updated to completely mitigate CVE-2016-5330.
References	http://www.vmware.com/security/advisories/VMSA-2016-0010.html http://kb.vmware.com/kb/2142193 http://kb.vmware.com/kb/2143976 http://kb.vmware.com/kb/2141429 http://kb.vmware.com/kb/2144359
Affected Nodes	192.168.2.5 on port 0/tcp 192.168.2.3 on port 0/tcp

Additional Output	`ESXi version : 5.1`
	`Installed build : 2000251`
	`Fixed build : 3872664 / 3872638 (security-only fix)`

ESXi 5.1 < Build 2323231 glibc Library Multiple Vulnerabilities (remote check)

Severity	
Description	The remote VMware ESXi host is version 5.1 prior to build 2323231. It is, therefore, affected by the following vulnerabilities in the glibc library : - A buffer overflow flaw exists in the 'extend_buffers' function of the 'posix/regexec.c' file due to improper validation of user input. Using a specially crafted expression, a remote attacker can cause a denial of service. (CVE-2013-0242) - A buffer overflow flaw exists in the 'getaddrinfo' function of the '/sysdeps/posix/getaddrinfo.c' file due to improper validation of user input. A remote attacker can cause a denial of service by triggering a large number of domain conversions. (CVE-2013-1914) The remote VMware ESXi 5.1 host is affected by multiple vulnerabilities.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)
Recommendation	Apply patch ESXi510-201412101-SG for ESXi 5.1.
References	https://www.vmware.com/security/advisories/VMSA-2014-0008.html
Affected Nodes	192.168.2.5 on port 0/tcp 192.168.2.3 on port 0/tcp

Additional Output	`ESXi version : ESXi 5.1`
	`Installed build : 2000251`
	`Fixed build : 2323231`

ESXi 5.1 < Build 2323236 Third-Party Libraries Multiple Vulnerabilities (remote check) (BEAST)

Severity	
Description	The remote VMware ESXi host is version 5.1 prior to build 2323236. It is, therefore, affected by the following vulnerabilities in bundled third-party libraries : - Multiple vulnerabilities exist in the bundled Python library. (CVE-2011-3389, CVE-2012-0845, CVE-2012-0876,

	CVE-2012-1150, CVE-2013-1752, CVE-2013-4238) - Multiple vulnerabilities exist in the bundled GNU C Library (glibc). (CVE-2013-0242, CVE-2013-1914, CVE-2013-4332) - Multiple vulnerabilities exist in the bundled XML Parser library (libxml2). (CVE-2013-2877, CVE-2014-0191) - Multiple vulnerabilities exist in the bundled cURL library (libcurl). (CVE-2014-0015, CVE-2014-0138) The remote VMware ESXi 5.1 host is affected by multiple vulnerabilities.
CVSS	6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)
Recommendation	Apply patch ESXi510-201412101-SG for ESXi 5.1.
References	http://www.nessus.org/u?5994bfcf https://www.vmware.com/security/advisories/VMSA-2014-0008.html https://www.vmware.com/security/advisories/VMSA-2014-0012.html
Affected Nodes	192.168.2.5 on port 0/tcp 192.168.2.3 on port 0/tcp

Additional Output	`ESXi version : ESXi 5.1`
	`Installed build : 2000251`
	`Fixed build : 2323236`

ESXi 5.1 < Build 3070626 Shared Folders (HGFS) Guest Privilege Escalation (VMSA-2016-0001) (remote check)

Severity	
Description	The remote VMware ESXi 5.1 host is prior to build 3070626. It is, therefore, affected by a guest privilege escalation vulnerability in the Shared Folders (HGFS) feature due to improper validation of user-supplied input. A local attacker can exploit this to corrupt memory, resulting in an elevation of privileges. The remote VMware ESXi 5.1 host is affected by a guest privilege escalation vulnerability.
CVSS	6.5 (CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:P)
CVSS3	6.3 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L)
Recommendation	Apply patch ESXi510-201510102-SG according to the vendor advisory. Note that VMware Tools in any Windows-based guests that use the Shared Folders (HGFS) feature must also be updated to completely mitigate the vulnerability.
References	http://www.vmware.com/security/advisories/VMSA-2016-0001.html http://www.nessus.org/u?c276b94f http://www.nessus.org/u?4cf0502f
Affected Nodes	192.168.2.5 on port 0/tcp 192.168.2.3 on port 0/tcp

Additional Output	`ESXi version : ESXi 5.1`
	`Installed build : 2000251`
	`Fixed build : 3070626`

HSTS Missing From HTTPS Server (RFC 6797)

Severity	
Description	The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections. The remote web server is not enforcing HSTS, as defined by RFC 6797.
CVSS	5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)
CVSS3	7.4 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)
Recommendation	Configure the remote web server to use HSTS.

References	https://tools.ietf.org/html/rfc6797
Affected Nodes	10.100.2.49 (IT09-H42HYV1) on port 443/tcp
Additional Output	The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.

HTTP TRACE / TRACK Methods Allowed

Severity	
Description	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. Debugging functions are enabled on the remote web server.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSS3	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
Recommendation	Disable these methods. Refer to the plugin output for more information.
References	https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf http://www.apacheweek.com/issues/03-01-24 https://download.oracle.com/sunalerts/1000718.1.html
Affected Nodes	192.168.2.51 on port 443/tcp 192.168.2.51 on port 80/tcp
Additional Output	To disable these methods, add the following lines for each virtual host in your configuration file : RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F] Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method natively via the 'TraceEnable' directive. vPenTest Partner sent the following TRACE request : ------------------------------ snip ------------------------------ TRACE /vPenTest Partner615465857.html HTTP/1.1 Connection: Close Host: 192.168.2.51 Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0) Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Accept-Language: en Accept-Charset: iso-8859-1,*,utf-8 ------------------------------ snip ------------------------------ and received the following response from the remote server : ------------------------------ snip ------------------------------ HTTP/1.1 200 OK Date: Mon, 11 Jan 2021 22:29:58 GMT ------------ snipped ------------

IP Forwarding Enabled

Severity	
Description	The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering. Unless the remote host is a router, it is recommended that you disable IP forwarding.

CVSS	5.8 (CVSS2#AV:A/AC:L/Au:N/C:P/I:P/A:P)
Recommendation	On Linux, you can disable IP forwarding by doing : echo 0 > /proc/sys/net/ipv4/ip_forward On Windows, set the key 'IPEnableRouter' to 0 under HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters On Mac OS X, you can disable IP forwarding by executing the command : sysctl -w net.inet.ip.forwarding=0 For other systems, check with your vendor.
References	n/a
Affected Nodes	10.100.2.62 on port 0/tcp 10.100.2.5 on port 0/tcp
Additional Output	`n/a`

JQuery 1.2 < 3.5.0 Multiple XSS

Severity	
Description	According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities. The remote web server is affected by multiple cross site scripting vulnerability.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)
CVSS3	6.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
Recommendation	Upgrade to JQuery version 3.5.0 or later.
References	https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
Affected Nodes	192.168.2.45 on port 80/tcp 10.100.31.66 on port 443/tcp 10.100.31.65 on port 443/tcp 10.100.31.64 on port 443/tcp 10.100.3.57 on port 443/tcp 10.100.1.74 on port 443/tcp

Additional Output	`URL              : http://192.168.2.45/base/js/jquery-1.6.2.min.js`
	`  Installed version : 1.6.2`
	`  Fixed version     : 3.5.0`

mDNS Detection (Remote Network)

Severity	
Description	The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running. This plugin attempts to discover mDNS used by hosts that are not on the network segment on which vPenTest Partner resides. It is possible to obtain information about the remote host.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
Recommendation	Filter incoming traffic to UDP port 5353, if desired.
References	n/a
Affected Nodes	10.100.35.50 on port 5353/udp

10.100.34.80 on port 5353/udp
10.100.34.72 on port 5353/udp
10.100.34.65 on port 5353/udp
10.100.34.63 on port 5353/udp
10.100.34.53 on port 5353/udp
10.100.34.50 on port 5353/udp
10.100.34.81 on port 5353/udp
10.100.34.79 on port 5353/udp
10.100.34.78 on port 5353/udp
10.100.34.77 on port 5353/udp
10.100.34.76 on port 5353/udp
10.100.34.75 on port 5353/udp
10.100.34.74 on port 5353/udp
10.100.34.73 on port 5353/udp
10.100.34.71 on port 5353/udp
10.100.34.70 on port 5353/udp
10.100.34.69 on port 5353/udp
10.100.34.68 on port 5353/udp
10.100.34.67 on port 5353/udp
10.100.34.66 on port 5353/udp
10.100.34.64 on port 5353/udp
10.100.34.62 on port 5353/udp
10.100.34.61 on port 5353/udp
10.100.34.60 on port 5353/udp
10.100.34.59 on port 5353/udp
10.100.34.58 on port 5353/udp
10.100.34.57 on port 5353/udp
10.100.34.56 on port 5353/udp
10.100.34.55 on port 5353/udp
10.100.34.54 on port 5353/udp
10.100.34.52 on port 5353/udp
10.100.34.51 on port 5353/udp
10.100.33.55 on port 5353/udp
10.100.32.62 on port 5353/udp
10.100.32.58 on port 5353/udp
10.100.32.56 on port 5353/udp
10.100.31.67 on port 5353/udp
10.100.33.50 on port 5353/udp
10.100.33.20 on port 5353/udp
10.100.32.69 on port 5353/udp
10.100.32.61 on port 5353/udp
10.100.32.59 on port 5353/udp
10.100.32.57 on port 5353/udp
10.100.32.55 on port 5353/udp
10.100.32.54 on port 5353/udp
10.100.32.53 on port 5353/udp
10.100.32.52 on port 5353/udp
10.100.32.51 on port 5353/udp
10.100.32.50 on port 5353/udp
10.100.31.82 on port 5353/udp
10.100.31.81 on port 5353/udp
10.100.31.80 on port 5353/udp
10.100.31.77 on port 5353/udp
10.100.31.75 on port 5353/udp
10.100.31.73 on port 5353/udp
10.100.31.71 on port 5353/udp
10.100.31.69 on port 5353/udp
10.100.31.60 on port 5353/udp
10.100.31.58 on port 5353/udp
10.100.31.56 on port 5353/udp
10.100.31.55 on port 5353/udp
10.100.31.54 on port 5353/udp
10.100.31.53 on port 5353/udp
10.100.31.52 on port 5353/udp
10.100.31.50 on port 5353/udp
10.100.7.150 on port 5353/udp
10.100.31.51 on port 5353/udp
10.100.6.87 on port 5353/udp
10.100.6.20 on port 5353/udp

	10.100.5.52 on port 5353/udp 10.100.3.151 on port 5353/udp 10.100.3.150 on port 5353/udp 10.100.5.53 on port 5353/udp 10.100.1.151 on port 5353/udp 10.100.1.150 on port 5353/udp

Additional Output	`vPenTest Partner was able to extract the following information :`
	
	`- mDNS hostname : UniFi-CloudKey-Gen2.local.`

Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

Severity	
Description	The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials. This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.
CVSS	5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)
Recommendation	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.
References	n/a
Affected Nodes	192.168.2.71 on port 3389/tcp 10.100.7.210 on port 3389/tcp 10.100.7.136 on port 3389/tcp 10.100.7.135 on port 3389/tcp 10.100.7.131 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.115 on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp 10.100.2.49 (IT09-H42HYV1) on port 3389/tcp
Additional Output	`n/a`

MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Severity	
Description	The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.
CVSS	5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)
CVSS3	6.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N)
Recommendation	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.
References	n/a
Affected Nodes	10.100.7.115 on port 49161/tcp 10.100.5.64 (CONMSAUTHMI601) on port 49156/tcp
Additional Output	`n/a`

OpenSSL 1.0.2 < 1.0.2k Multiple Vulnerabilities

Severity	
Description	According to its banner, the version of OpenSSL running on the remote host is 1.0.2 prior to 1.0.2k. It is, therefore, affected by multiple vulnerabilities : - A carry propagation error exists in the Broadwell-specific Montgomery multiplication procedure when handling input lengths divisible by but longer than 256 bits. This can result in transient authentication and key negotiation failures or reproducible erroneous outcomes of public-key operations with specially crafted input. A man-in-the-middle attacker can possibly exploit this issue to compromise ECDH key negotiations that utilize Brainpool P-512 curves. (CVE-2016-7055) - An out-of-bounds read error exists when handling packets using the CHACHA20/POLY1305 or RC4-MD5 ciphers. An unauthenticated, remote attacker can exploit this, via specially crafted truncated packets, to cause a denial of service condition. (CVE-2017-3731) - A carry propagating error exists in the x86_64 Montgomery squaring implementation that may cause the BN_mod_exp() function to produce incorrect results. An unauthenticated, remote attacker with sufficient resources can exploit this to obtain sensitive information regarding private keys. Note that this issue is very similar to CVE-2015-3193. Moreover, the attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. For example, this can occur by default in OpenSSL DHE based SSL/TLS cipher suites. (CVE-2017-3732) A service running on the remote host is affected by multiple vulnerabilities.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Upgrade to OpenSSL version 1.0.2k or later.
References	https://www.openssl.org/news/secadv/20170126.txt
Affected Nodes	10.100.6.87 on port 80/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2k`

OpenSSL 1.0.2 < 1.0.2n Multiple Vulnerabilities

Severity	
Description	According to its banner, the version of OpenSSL running on the remote host is 1.0.x prior to 1.0.2n. It is, therefore, affected by multiple vulnerabilities that allow potential recovery of private key information or failure to properly encrypt data. A service running on the remote host is affected by multiple vulnerabilities.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Upgrade to OpenSSL version 1.0.2n or later.
References	https://www.openssl.org/news/secadv/20171207.txt
Affected Nodes	10.100.6.87 on port 80/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2n`

OpenSSL 1.0.2 < 1.0.2u Procedure Overflow Vulnerability

Severity	
Description	The version of OpenSSL installed on the remote host is prior to 1.0.2u. It is, therefore, affected by a vulnerability as referenced in the 1.0.2u advisory.

	- There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e-dev (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u-dev (Affected 1.0.2-1.0.2t). (CVE-2019-1551) Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote service is affected by a procedure overflow vulnerability.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSS3	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
Recommendation	Upgrade to OpenSSL version 1.0.2u or later.
References	http://www.nessus.org/u?83f0f491 https://www.openssl.org/news/secadv/20191206.txt
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 80/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2u-dev`

OpenSSL 1.0.2 < 1.0.2x Null Pointer Dereference Vulnerability

Severity	
Description	The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the 1.0.2x advisory. - The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the -crl_download option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w). (CVE-2020-1971) Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote service is affected by a null pointer dereference vulnerability.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)
CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
Recommendation	Upgrade to OpenSSL version 1.0.2x or later.
References	http://www.nessus.org/u?101e8ed5

	https://www.openssl.org/news/secadv/20201208.txt
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 80/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2x`

OpenSSL 1.0.x < 1.0.2m RSA/DSA Unspecified Carry Issue

Severity	
Description	According to its banner, the version of OpenSSL running on the remote host is 1.0.x prior to 1.0.2m. It is, therefore, affected by an unspecified carry vulnerability. A service running on the remote host is affected by an unspecified carry vulnerability.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS3	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
Recommendation	Upgrade to OpenSSL version 1.0.2m or later.
References	https://www.openssl.org/news/secadv/20171102.txt
Affected Nodes	10.100.6.87 on port 80/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2m`

OpenSSL 1.0.x < 1.0.2o Multiple Vulnerabilities

Severity	
Description	According to its banner, the version of OpenSSL running on the remote host is 1.0.x prior to 1.0.2o. It is, therefore, affected by a remote DoS vulnerability. A service running on the remote host is affected by multiple vulnerabilities.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)
CVSS3	6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)
Recommendation	Upgrade to OpenSSL version 1.0.2o or later.
References	https://www.openssl.org/news/secadv/20180327.txt https://www.openssl.org/news/openssl-1.0.2-notes.html
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2o`

OpenSSL 1.0.x < 1.0.2p Multiple Vulnerabilities

Severity	
Description	According to its banner, the version of OpenSSL running on the remote host is 1.0.x prior to 1.0.2p. It is, therefore, affected by a denial of service vulnerability and a cache timing side channel vulnerability. A service running on the remote host is affected by multiple vulnerabilities.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Upgrade to OpenSSL version 1.0.2p or later.
References	https://www.openssl.org/news/secadv/20180612.txt https://www.openssl.org/news/secadv/20180416.txt
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2p`

OpenSSL 1.0.x < 1.0.2q Multiple Vulnerabilities

Severity	
Description	According to its banner, the version of OpenSSL running on the remote host is 1.0.x prior to 1.0.2q. It is, therefore, affected by a denial of service vulnerability and a cache timing side channel vulnerability. A service running on the remote host is affected by multiple vulnerabilities.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Upgrade to OpenSSL version 1.0.2q or later.
References	https://www.openssl.org/news/secadv/20181112.txt https://www.openssl.org/news/secadv/20181030.txt
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 80/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2q`

OpenSSL 1.0.x < 1.0.2r Information Disclosure Vulnerability

Severity	
Description	According to its banner, the version of OpenSSL running on the remote host is 1.0.x prior to 1.0.2r. It is, therefore, affected by an information disclosure vulnerability due to the decipherable way a application responds to a 0 byte record. An unauthenticated, remote attacker could exploit this vulnerability, via a padding oracle attack, to potentially disclose sensitive information. Note: Only 'non-stitched' ciphersuites are exploitable. A service running on the remote host is affected by an information disclosure vulnerability.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Upgrade to OpenSSL version 1.0.2r or later.
References	http://www.nessus.org/u?0e8c6acd https://www.openssl.org/news/secadv/20190226.txt
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 443/tcp 10.100.6.20 on port 80/tcp

Additional Output	`Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j`
	`Reported version : 1.0.2j`
	`Fixed version : 1.0.2r`

OpenSSL 1.1.1 < 1.1.1e-dev Procedure Overflow Vulnerability	
Severity	
Description	The version of OpenSSL installed on the remote host is prior to 1.1.1e-dev. It is, therefore, affected by a vulnerability as referenced in the 1.1.1e-dev advisory. - There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e-dev (Affected 1.1.1-1.1.1d). (CVE-2019-1551) Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote service is affected by a procedure overflow vulnerability.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSS3	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
Recommendation	Upgrade to OpenSSL version 1.1.1e-dev or later.
References	http://www.nessus.org/u?83f0f491 https://www.openssl.org/news/secadv/20191206.txt
Affected Nodes	10.100.31.82 on port 80/tcp 10.100.31.81 on port 443/tcp 10.100.31.81 on port 80/tcp 10.100.31.69 on port 443/tcp 10.100.31.69 on port 80/tcp 10.100.31.52 on port 443/tcp 10.100.31.82 on port 443/tcp 10.100.31.60 on port 443/tcp 10.100.31.60 on port 80/tcp 10.100.31.54 on port 443/tcp 10.100.31.54 on port 80/tcp 10.100.31.52 on port 80/tcp

Additional Output	`Banner           : Apache/2.4.41 (Unix) OpenSSL/1.1.1d`
	`  Reported version : 1.1.1d`
	`  Fixed version    : 1.1.1e-dev`

OpenSSL 1.1.1 < 1.1.1g Vulnerability	
Severity	
Description	The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the 1.1.1g advisory. - Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the signature_algorithms_cert TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affect OpenSSL versions prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected 1.1.1d-1.1.1f). (CVE-2020-1967) Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote service is affected by a vulnerability.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Recommendation	Upgrade to OpenSSL version 1.1.1g or later.
References	http://www.nessus.org/u?5929f842 https://www.openssl.org/news/secadv/20200421.txt
Affected Nodes	10.100.31.82 on port 443/tcp 10.100.31.82 on port 80/tcp 10.100.31.81 on port 443/tcp 10.100.31.81 on port 80/tcp 10.100.31.69 on port 80/tcp 10.100.31.69 on port 443/tcp 10.100.31.60 on port 443/tcp 10.100.31.60 on port 80/tcp 10.100.31.54 on port 443/tcp 10.100.31.54 on port 80/tcp 10.100.31.52 on port 443/tcp 10.100.31.52 on port 80/tcp

Additional Output	`Banner : Apache/2.4.41 (Unix) OpenSSL/1.1.1d`
	`Reported version : 1.1.1d`
	`Fixed version : 1.1.1g`

OpenSSL 1.1.1 < 1.1.1i Null Pointer Dereference Vulnerability

Severity	
Description	The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the 1.1.1i advisory. - The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the -crl_download option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w). (CVE-2020-1971) Note that vPenTest Partner has not tested for this issue but has instead relied only on the application's self-reported version number. The remote service is affected by a null pointer dereference vulnerability.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)
CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
Recommendation	Upgrade to OpenSSL version 1.1.1i or later.
References	http://www.nessus.org/u?dc9b62cf https://www.openssl.org/news/secadv/20201208.txt
Affected Nodes	10.100.31.82 on port 443/tcp 10.100.31.82 on port 80/tcp 10.100.31.81 on port 443/tcp 10.100.31.69 on port 443/tcp 10.100.31.69 on port 80/tcp 10.100.31.60 on port 443/tcp 10.100.31.60 on port 80/tcp

	10.100.31.81 on port 80/tcp 10.100.31.54 on port 443/tcp 10.100.31.54 on port 80/tcp 10.100.31.52 on port 443/tcp 10.100.31.52 on port 80/tcp

Additional Output	`Banner : Apache/2.4.41 (Unix) OpenSSL/1.1.1d`
	`Reported version : 1.1.1d`
	`Fixed version : 1.1.1i`

Rockwell Automation FactoryTalk Linx Path Traversal Information Disclosure

Severity	
Description	The Rockwell Automation FactoryTalk Linx running on the remote host is affected by a path traversal vulnerability due to the lack of validation of user-supplied file paths before using them in file operations. An unauthenticated, remote attacker can exploit this, via specially crafted messages, to disclose the contents of files on the remote host with SYSTEM privileges. This plugin requires the 'Scan Operational Technology devices' scan setting to be enabled for it to be launched. Note that the application is reportedly affected by other vulnerabilities; however, this plugin has not tested for those issues. The remote SCADA application is affected by an information disclosure vulnerability.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Apply Patch Aid 1124820 or the May 2020 Patch Roll-up or later.
References	http://www.nessus.org/u?8ad24a10
Affected Nodes	10.100.7.93 (OWS-01A) on port 7153/tcp 10.100.7.77 (HMI-01A) on port 7153/tcp 10.100.7.70 (EWS-01) on port 7153/tcp

Additional Output	`vPenTest Partner was able to exploit the issue to download the contents of \Windows\win.ini on the di sk drive where the EDS icon folder is installed :`
	
	`; for 16-bit app support`
	`[fonts]`
	`[extensions]`
	`[mci extensions]`
	`[files]`
	`[Mail]`
	`MAPI=1`

SMB Signing not required

Severity	
Description	Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS3	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
Recommendation	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
References	n/a
Affected Nodes	192.168.2.93 on port 445/tcp 192.168.2.84 on port 445/tcp 192.168.2.82 on port 445/tcp 192.168.2.78 on port 445/tcp 192.168.2.74 on port 445/tcp

192.168.2.91 on port 445/tcp
192.168.2.85 on port 445/tcp
192.168.2.22 on port 445/tcp
192.168.2.19 on port 445/tcp
192.168.2.8 on port 445/tcp
10.100.35.119 on port 445/tcp
10.100.35.89 on port 445/tcp
10.100.35.77 on port 445/tcp
192.168.2.25 on port 445/tcp
10.100.35.72 on port 445/tcp
10.100.34.86 on port 445/tcp
10.100.34.85 on port 445/tcp
10.100.34.83 on port 445/tcp
10.100.33.59 on port 445/tcp
10.100.33.54 on port 445/tcp
10.100.33.53 on port 445/tcp
10.100.32.65 on port 445/tcp
10.100.32.63 on port 445/tcp
10.100.31.70 on port 445/tcp
10.100.31.61 on port 445/tcp
10.100.31.59 on port 445/tcp
10.100.20.200 on port 445/tcp
10.100.20.195 on port 445/tcp
10.100.20.145 on port 445/tcp
10.100.20.38 (ssd505) on port 445/tcp
10.100.20.33 (lt186) on port 445/tcp
10.100.20.11 on port 445/tcp
10.100.20.2 on port 445/tcp
10.100.7.210 on port 445/tcp
10.100.7.201 on port 445/tcp
10.100.7.136 on port 445/tcp
10.100.7.135 on port 445/tcp
10.100.7.131 on port 445/tcp
10.100.7.125 on port 445/tcp
10.100.7.119 on port 445/tcp
10.100.7.118 on port 445/tcp
10.100.7.116 on port 445/tcp
10.100.7.115 on port 445/tcp
10.100.7.111 on port 445/tcp
10.100.7.110 on port 445/tcp
10.100.7.101 (SmartTool-TMP) on port 445/tcp
10.100.20.7 on port 445/tcp
10.100.7.90 (HMI-01B) on port 445/tcp
10.100.7.88 (URSIOSSVR01) on port 445/tcp
10.100.7.87 (SmartTool) on port 445/tcp
10.100.7.86 (HIST-01A) on port 445/tcp
10.100.7.85 (MPM) on port 445/tcp
10.100.7.84 (HMI1) on port 445/tcp
10.100.7.82 (TESTPC06) on port 445/tcp
10.100.7.78 (OSSEM3_RIUHMI01) on port 445/tcp
10.100.7.77 (HMI-01A) on port 445/tcp
10.100.7.75 (IT03-5D3BVV1) on port 445/tcp
10.100.7.73 (VSS-01A) on port 445/tcp
10.100.7.72 (DESKTOP-KOCHTQC) on port 445/tcp
10.100.7.71 (VSS-01B) on port 445/tcp
10.100.7.70 (EWS-01) on port 445/tcp
10.100.7.66 (URSIOSSVR02) on port 445/tcp
10.100.7.62 (OSSEM2_RIOHMI01) on port 445/tcp
10.100.7.53 (URSHISTSVR01) on port 445/tcp
10.100.7.51 (it03-8ddvdv1) on port 445/tcp
10.100.7.50 (IT02-8ZWM353) on port 445/tcp
10.100.6.92 (IT01-1K7FLR2) on port 445/tcp
10.100.6.90 (IT01-FT0Y4Y2) on port 445/tcp
10.100.6.84 (IT01-G9S2YM2) on port 445/tcp
10.100.6.81 (IT01-CX9WNW1) on port 445/tcp
10.100.6.80 (IT01-486J8V1-Wiring-PC) on port 445/tcp
10.100.6.69 (IT01-9WQ7HD1) on port 445/tcp
10.100.6.68 (IT01-CMCW8Y1) on port 445/tcp
10.100.6.66 (IT01-GS97L02) on port 445/tcp

	10.100.6.65 (IT01-B11Y4Y2) on port 445/tcp 10.100.6.62 (IT01-486G8V1) on port 445/tcp 10.100.6.60 (IT01-2VDFG12) on port 445/tcp 10.100.6.57 (IT01-8WWKQ13) on port 445/tcp 10.100.6.53 (IT01-8NQH353) on port 445/tcp 10.100.6.50 (IT02-FGXJ842) on port 445/tcp 10.100.5.68 (IT02-2SD5Y2) on port 445/tcp 10.100.5.67 (IT02-4RWKQ13) on port 445/tcp 10.100.5.64 (CONMSAUTHMI601) on port 445/tcp 10.100.5.62 (IT02-DWCKN53) on port 445/tcp 10.100.5.61 (IT02-34HR733) on port 445/tcp 10.100.5.60 (IT08-DF9HLW2) on port 445/tcp 10.100.5.59 (IT06-G8F8HF1) on port 445/tcp 10.100.5.56 (IT02-GS5WZY2) on port 445/tcp 10.100.5.55 (IT09-5Z5KN53) on port 445/tcp 10.100.3.64 (IT01-4P775Y2) on port 445/tcp 10.100.3.56 (IT02-FNFR2R1) on port 445/tcp 10.100.3.51 (IT03-4M7MM32) on port 445/tcp 10.100.2.93 (IT10-DHVDT13) on port 445/tcp 10.100.2.83 (Training2) on port 445/tcp 10.100.2.82 (Training8) on port 445/tcp 10.100.2.70 (IT09-6GRJN53) on port 445/tcp 10.100.2.66 (IT10-34S1MQ1) on port 445/tcp 10.100.2.65 (IT09-JGYQ733) on port 445/tcp 10.100.2.64 (it10-g0wtsw1) on port 445/tcp 10.100.2.63 (WIN-NLN1IU84VKS) on port 445/tcp 10.100.2.59 (WIN-NLN1IU84VKS) on port 445/tcp 10.100.2.55 (Training3) on port 445/tcp 10.100.2.53 (it05-100625) on port 445/tcp 10.100.2.52 (WIN-NLN1IU84VKS) on port 445/tcp 10.100.2.49 (IT09-H42HYV1) on port 445/tcp 10.100.1.99 (IT10-BVMFJX2) on port 445/tcp 10.100.1.97 (IT10-37HWTR1) on port 445/tcp 10.100.1.76 (IT10-F8BP2R1) on port 445/tcp 10.100.1.68 (IT10-F20GXV1) on port 445/tcp 10.100.1.66 (IT10--HNGWST2) on port 445/tcp
Additional Output	n/a

SNMP 'GETBULK' Reflection DDoS	
Severity	
Description	The remote SNMP daemon is responding with a large amount of data to a 'GETBULK' request with a larger than normal value for 'max-repetitions'. A remote attacker can use this SNMP server to conduct a reflected distributed denial of service attack on an arbitrary remote host. The remote SNMP daemon is affected by a vulnerability that allows a reflected distributed denial of service attack.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)
Recommendation	Disable the SNMP service on the remote host if you do not use it. Otherwise, restrict and monitor access to this service, and consider changing the default 'public' community string.
References	http://www.nessus.org/u?8b551b5c http://www.nessus.org/u?bdb53cfc
Affected Nodes	192.168.2.58 on port 161/udp 192.168.2.57 on port 161/udp 192.168.2.55 on port 161/udp 192.168.2.20 on port 161/udp 192.168.2.14 on port 161/udp 192.168.2.2 on port 161/udp 192.168.2.28 on port 161/udp 10.100.7.68 on port 161/udp 10.100.7.67 on port 161/udp 10.100.7.64 on port 161/udp 10.100.7.63 on port 161/udp

Additional Output	vPenTest Partner was able to determine the SNMP service can be abused in an SNMP Reflection DDoS attack : Request size (bytes) : 42 Response size (bytes) : 2312

SSH Weak Algorithms Supported

Severity	
Description	vPenTest Partner has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys. The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
Recommendation	Contact the vendor or consult product documentation to remove the weak ciphers.
References	https://tools.ietf.org/html/rfc4253#section-6.3
Affected Nodes	10.100.7.74 on port 22/tcp
Additional Output	The following weak server-to-client encryption algorithms are supported : arcfour arcfour128 The following weak client-to-server encryption algorithms are supported : arcfour arcfour128

SSL Certificate Cannot Be Trusted

Severity	
Description	The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below : - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority. - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that vPenTest Partner either does not support or does not recognize. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. The SSL certificate for this service cannot be trusted.
CVSS	6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)
CVSS3	6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
Recommendation	Purchase or generate a proper certificate for this service.
References	https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509
Affected Nodes	192.168.2.74 on port 3389/tcp 192.168.2.71 on port 3389/tcp

192.168.2.64 on port 443/tcp
192.168.2.61 on port 443/tcp
192.168.2.60 on port 443/tcp
192.168.2.59 on port 443/tcp
192.168.2.58 on port 443/tcp
192.168.2.94 on port 631/tcp
192.168.2.82 on port 3389/tcp
192.168.2.78 on port 3389/tcp
192.168.2.63 on port 443/tcp
192.168.2.57 on port 443/tcp
192.168.2.56 on port 443/tcp
192.168.2.55 on port 443/tcp
192.168.2.51 on port 443/tcp
192.168.2.22 on port 3389/tcp
192.168.2.18 on port 54433/tcp
192.168.2.8 on port 1433/tcp
192.168.2.8 on port 3389/tcp
192.168.2.8 on port 2002/tcp
192.168.2.6 on port 3389/tcp
192.168.2.5 on port 443/tcp
192.168.2.3 on port 5989/tcp
192.168.2.3 on port 443/tcp
10.100.35.119 on port 3389/tcp
10.100.35.104 on port 443/tcp
10.100.35.101 on port 443/tcp
10.100.35.89 on port 3389/tcp
10.100.35.87 on port 443/tcp
10.100.35.73 on port 3001/tcp
192.168.2.18 on port 3389/tcp
192.168.2.5 on port 902/tcp
192.168.2.5 on port 5989/tcp
192.168.2.3 on port 902/tcp
10.100.35.113 on port 443/tcp
10.100.35.51 on port 443/tcp
10.100.35.50 on port 443/tcp
10.100.34.85 on port 3389/tcp
10.100.34.65 on port 443/tcp
10.100.33.61 on port 3389/tcp
10.100.33.59 on port 3389/tcp
10.100.34.80 on port 443/tcp
10.100.33.54 on port 3389/tcp
10.100.33.52 on port 443/tcp
10.100.31.82 on port 443/tcp
10.100.31.81 on port 443/tcp
10.100.31.66 on port 443/tcp
10.100.31.65 on port 443/tcp
10.100.32.65 on port 3389/tcp
10.100.31.69 on port 443/tcp
10.100.31.69 on port 5061/tcp
10.100.31.64 on port 443/tcp
10.100.31.60 on port 443/tcp
10.100.31.54 on port 443/tcp
10.100.31.52 on port 443/tcp
10.100.20.200 on port 1433/tcp
10.100.20.33 (lt186) on port 3389/tcp
10.100.7.210 on port 3389/tcp
10.100.7.210 on port 3071/tcp
10.100.7.201 on port 3389/tcp
10.100.7.131 on port 3389/tcp
10.100.7.125 on port 3389/tcp
10.100.7.119 on port 1433/tcp
10.100.7.118 on port 3389/tcp
10.100.7.116 on port 1433/tcp
10.100.7.115 on port 3389/tcp
10.100.7.111 on port 3071/tcp
10.100.7.110 on port 3389/tcp
10.100.7.98 on port 443/tcp
10.100.7.97 on port 443/tcp
10.100.7.96 on port 9080/tcp

	10.100.7.96 on port 443/tcp 10.100.7.135 on port 3389/tcp 10.100.7.95 (IT09-5Z5KN53) on port 9080/tcp 10.100.7.95 (IT09-5Z5KN53) on port 443/tcp 10.100.7.88 (URSIOSSVR01) on port 3389/tcp 10.100.7.86 (HIST-01A) on port 1433/tcp 10.100.7.85 (MPM) on port 1433/tcp 10.100.7.84 (HMI1) on port 3389/tcp 10.100.7.82 (TESTPC06) on port 3389/tcp 10.100.7.78 (OSSEM3_RIUHMI01) on port 3389/tcp 10.100.7.75 (IT03-5D3BVV1) on port 3389/tcp 10.100.7.74 on port 443/tcp 10.100.7.73 (VSS-01A) on port 1433/tcp 10.100.7.72 (DESKTOP-KOCHTQC) on port 3389/tcp 10.100.7.71 (VSS-01B) on port 1433/tcp 10.100.7.69 on port 443/tcp 10.100.7.66 (URSIOSSVR02) on port 3389/tcp 10.100.7.62 (OSSEM2_RIOHMI01) on port 3389/tcp 10.100.7.53 (URSHISTSVR01) on port 1433/tcp 10.100.7.53 (URSHISTSVR01) on port 3389/tcp 10.100.7.51 (it03-8ddvdv1) on port 3389/tcp 10.100.6.90 (IT01-FT0Y4Y2) on port 3389/tcp 10.100.6.81 (IT01-CX9WNW1) on port 3389/tcp 10.100.6.65 (IT01-B11Y4Y2) on port 3389/tcp 10.100.6.20 on port 443/tcp 10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp 10.100.5.68 (IT02-2SD5Y2) on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp 10.100.5.60 (IT08-DF9HLW2) on port 3389/tcp 10.100.5.58 on port 443/tcp 10.100.3.64 (IT01-4P775Y2) on port 3389/tcp 10.100.3.57 on port 443/tcp 10.100.3.52 (IT10-CM1V8Y1) on port 3389/tcp 10.100.3.51 (IT03-4M7MM32) on port 3389/tcp 10.100.2.93 (IT10-DHVDT13) on port 3389/tcp 10.100.2.81 (WindUtilWS) on port 3389/tcp 10.100.2.70 (IT09-6GRJN53) on port 443/tcp 10.100.2.60 on port 9080/tcp 10.100.2.60 on port 443/tcp 10.100.2.58 on port 9080/tcp 10.100.2.58 on port 443/tcp 10.100.2.57 on port 9080/tcp 10.100.2.57 on port 443/tcp 10.100.2.56 on port 9080/tcp 10.100.2.56 on port 443/tcp 10.100.2.54 (IT09-1KBKLR2) on port 3389/tcp 10.100.2.53 (it05-100625) on port 3389/tcp 10.100.2.53 (it05-100625) on port 8191/tcp 10.100.2.53 (it05-100625) on port 8089/tcp 10.100.2.51 on port 8834/tcp 10.100.2.49 (IT09-H42HYV1) on port 3389/tcp 10.100.2.49 (IT09-H42HYV1) on port 443/tcp 10.100.2.45 on port 8443/tcp 10.100.2.45 on port 443/tcp 10.100.1.151 on port 443/tcp 10.100.1.150 on port 443/tcp 10.100.1.99 (IT10-BVMFJX2) on port 3389/tcp 10.100.1.80 on port 8009/tcp 10.100.1.80 on port 8443/tcp 10.100.1.76 (IT10-F8BP2R1) on port 3389/tcp 10.100.1.74 on port 443/tcp
Additional Output	The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority : |-Subject : CN=shipping-imac.local |-Issuer : CN=shipping-imac.local

SSL Certificate Expiry	
Severity	
Description	This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired. The remote server's SSL certificate has already expired.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS3	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
Recommendation	Purchase or generate a new SSL certificate to replace the existing one.
References	n/a
Affected Nodes	192.168.2.51 on port 443/tcp 10.100.7.210 on port 3071/tcp 10.100.7.111 on port 3071/tcp

Additional Output	`The SSL certificate has already expired :`
	
	`Subject : C=US, ST=Texas, L=Houston, O=Volta LLC, CN=volta-us, emailAddress=charles.hopper@volta-us.com`
	`Issuer : C=US, ST=Texas, L=Houston, O=Volta LLC, CN=volta-us, emailAddress=charles.hopper@volta-us.com`
	`Not valid before : May 24 19:18:41 2017 GMT`
	`Not valid after : May 24 19:18:41 2018 GMT`

SSL Certificate Signed Using Weak Hashing Algorithm	
Severity	
Description	The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm. Note that certificates in the chain that are contained in the vPenTest Partner CA database (known_CA.inc) have been ignored. An SSL certificate in the certificate chain has been signed using a weak hash algorithm.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
Recommendation	Contact the Certificate Authority to have the certificate reissued.
References	https://tools.ietf.org/html/rfc3279 http://www.nessus.org/u?9bb87bf2 http://www.nessus.org/u?e120eea1 http://www.nessus.org/u?5d894816 http://www.nessus.org/u?51db68aa http://www.nessus.org/u?9dc7bfba
Affected Nodes	192.168.2.64 on port 443/tcp 192.168.2.61 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.59 on port 443/tcp 192.168.2.57 on port 443/tcp 192.168.2.55 on port 443/tcp 192.168.2.51 on port 443/tcp 192.168.2.63 on port 443/tcp 192.168.2.58 on port 443/tcp 192.168.2.56 on port 443/tcp

	192.168.2.18 on port 54433/tcp 192.168.2.3 on port 443/tcp 192.168.2.5 on port 902/tcp 192.168.2.5 on port 5989/tcp 192.168.2.5 on port 443/tcp 192.168.2.3 on port 902/tcp 192.168.2.3 on port 5989/tcp 10.100.20.200 on port 1433/tcp 10.100.7.210 on port 3389/tcp 10.100.7.210 on port 3071/tcp 10.100.7.135 on port 3389/tcp 10.100.7.131 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.119 on port 1433/tcp 10.100.7.116 on port 1433/tcp 10.100.7.115 on port 3389/tcp 10.100.7.111 on port 3071/tcp 10.100.7.86 (HIST-01A) on port 1433/tcp 10.100.7.85 (MPM) on port 1433/tcp 10.100.7.71 (VSS-01B) on port 1433/tcp 10.100.7.73 (VSS-01A) on port 1433/tcp 10.100.7.53 (URSHISTSVR01) on port 1433/tcp 10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp 10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp

Additional Output	`The following certificates were part of the certificate chain sent by`
	`the remote host, but contain hashes that are considered to be weak.`
	
	`|-Subject : C=US/ST=California/L=Sunnyvale/O=Ruckus Wireless Inc/CN=Ruckus Wireless Inc. SN-431204006316`
	`|-Signature Algorithm : SHA-1 With RSA Encryption`
	`|-Valid From : Sep 10 06:34:18 2012 GMT`
	`|-Valid To : Sep 18 06:34:18 2037 GMT`

SSL Certificate with Wrong Hostname	
Severity	
Description	The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. The SSL certificate for this service is for a different host.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS3	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
Recommendation	Purchase or generate a proper certificate for this service.
References	n/a
Affected Nodes	192.168.2.78 on port 3389/tcp 192.168.2.74 on port 3389/tcp 192.168.2.22 on port 3389/tcp 192.168.2.19 on port 3389/tcp 192.168.2.18 on port 54433/tcp 192.168.2.18 on port 3389/tcp 192.168.2.8 on port 1433/tcp 192.168.2.8 on port 3389/tcp 192.168.2.6 on port 3389/tcp 192.168.2.22 on port 443/tcp 192.168.2.19 on port 443/tcp 10.100.20.200 on port 1433/tcp 10.100.7.210 on port 3071/tcp 10.100.7.119 on port 1433/tcp 10.100.7.116 on port 1433/tcp 10.100.7.111 on port 3071/tcp 10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp 10.100.2.70 (IT09-6GRJN53) on port 443/tcp 10.100.2.53 (it05-100625) on port 8191/tcp

	10.100.2.53 (it05-100625) on port 8089/tcp 10.100.2.51 on port 8834/tcp
Additional Output	The identities known by vPenTest Partner are : 192.168.2.78 192.168.2.78 The Common Name in the certificate is : WIRESHOP.ad.volta-us.com

SSL Medium Strength Cipher Suites Supported (SWEET32)	
Severity	
Description	The remote host supports the use of SSL ciphers that offer medium strength encryption. vPenTest Partner regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network. The remote service supports the use of medium strength SSL ciphers.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSS3	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Reconfigure the affected application if possible to avoid use of medium strength ciphers.
References	https://www.openssl.org/blog/blog/2016/08/24/sweet32/ https://sweet32.info
Affected Nodes	192.168.2.71 on port 3389/tcp 192.168.2.64 on port 443/tcp 192.168.2.61 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.59 on port 443/tcp 192.168.2.58 on port 443/tcp 192.168.2.58 on port 1883/tcp 192.168.2.57 on port 1883/tcp 192.168.2.57 on port 443/tcp 192.168.2.56 on port 1883/tcp 192.168.2.55 on port 443/tcp 192.168.2.78 on port 3389/tcp 192.168.2.74 on port 3389/tcp 192.168.2.63 on port 443/tcp 192.168.2.56 on port 443/tcp 192.168.2.55 on port 1883/tcp 192.168.2.51 on port 443/tcp 10.100.35.89 on port 3389/tcp 10.100.35.87 on port 443/tcp 192.168.2.19 on port 3389/tcp 192.168.2.19 on port 443/tcp 192.168.2.18 on port 54433/tcp 192.168.2.18 on port 3389/tcp 192.168.2.8 on port 1433/tcp 192.168.2.8 on port 3389/tcp 192.168.2.6 on port 3389/tcp 192.168.2.5 on port 5989/tcp 192.168.2.3 on port 5989/tcp 10.100.35.119 on port 3389/tcp 10.100.35.113 on port 443/tcp 10.100.35.104 on port 443/tcp 10.100.35.101 on port 443/tcp 10.100.35.51 on port 443/tcp 10.100.34.85 on port 3389/tcp 10.100.34.80 on port 443/tcp 10.100.34.65 on port 443/tcp

	10.100.33.61 on port 3389/tcp 10.100.33.59 on port 3389/tcp 10.100.33.52 on port 443/tcp 10.100.32.65 on port 3389/tcp 10.100.33.54 on port 3389/tcp 10.100.20.200 on port 1433/tcp 10.100.20.33 (lt186) on port 3389/tcp 10.100.7.210 on port 3071/tcp 10.100.7.201 on port 3389/tcp 10.100.7.116 on port 1433/tcp 10.100.7.115 on port 3389/tcp 10.100.7.111 on port 3071/tcp 10.100.7.110 on port 3389/tcp 10.100.7.210 on port 3389/tcp 10.100.7.135 on port 3389/tcp 10.100.7.131 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.119 on port 1433/tcp 10.100.7.118 on port 3389/tcp 10.100.7.86 (HIST-01A) on port 1433/tcp 10.100.7.85 (MPM) on port 1433/tcp 10.100.7.84 (HMI1) on port 3389/tcp 10.100.7.82 (TESTPC06) on port 3389/tcp 10.100.7.75 (IT03-5D3BVV1) on port 3389/tcp 10.100.7.73 (VSS-01A) on port 1433/tcp 10.100.7.72 (DESKTOP-KOCHTQC) on port 3389/tcp 10.100.7.66 (URSIOSSVR02) on port 3389/tcp 10.100.7.62 (OSSEM2_RIOHMI01) on port 3389/tcp 10.100.7.53 (URSHISTSVR01) on port 1433/tcp 10.100.7.53 (URSHISTSVR01) on port 3389/tcp 10.100.7.51 (it03-8ddvdv1) on port 3389/tcp 10.100.6.90 (IT01-FT0Y4Y2) on port 3389/tcp 10.100.7.88 (URSIOSSVR01) on port 3389/tcp 10.100.6.65 (IT01-B11Y4Y2) on port 3389/tcp 10.100.7.78 (OSSEM3_RIUHMI01) on port 3389/tcp 10.100.7.71 (VSS-01B) on port 1433/tcp 10.100.6.81 (IT01-CX9WNW1) on port 3389/tcp 10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp 10.100.5.68 (IT02-2SD5Y2) on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp 10.100.5.60 (IT08-DF9HLW2) on port 3389/tcp 10.100.3.64 (IT01-4P775Y2) on port 3389/tcp 10.100.3.52 (IT10-CM1V8Y1) on port 3389/tcp 10.100.3.51 (IT03-4M7MM32) on port 3389/tcp 10.100.2.93 (IT10-DHVDT13) on port 3389/tcp 10.100.2.54 (IT09-1KBKLR2) on port 3389/tcp 10.100.2.53 (it05-100625) on port 3389/tcp 10.100.2.49 (IT09-H42HYV1) on port 3389/tcp 10.100.1.99 (IT10-BVMFJX2) on port 3389/tcp 10.100.2.81 (WindUtilWS) on port 3389/tcp 10.100.1.80 on port 8009/tcp 10.100.1.76 (IT10-F8BP2R1) on port 3389/tcp
Additional Output	Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES) Name Code KEX Auth Encryption MAC DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1 The fields above are : {Tenable ciphername} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryption method} MAC={message authentication code} {export flag}

SSL Self-Signed Certificate	
Severity	
Description	The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host. Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. The SSL certificate chain for this service ends in an unrecognized self-signed certificate.
CVSS	6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)
Recommendation	Purchase or generate a proper certificate for this service.
References	n/a
Affected Nodes	192.168.2.78 on port 3389/tcp 192.168.2.74 on port 3389/tcp 192.168.2.71 on port 3389/tcp 192.168.2.64 on port 443/tcp 192.168.2.63 on port 443/tcp 192.168.2.61 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.59 on port 443/tcp 192.168.2.58 on port 443/tcp 192.168.2.57 on port 443/tcp 192.168.2.55 on port 443/tcp 192.168.2.51 on port 443/tcp 192.168.2.94 on port 631/tcp 192.168.2.82 on port 3389/tcp 192.168.2.56 on port 443/tcp 192.168.2.18 on port 3389/tcp 192.168.2.8 on port 3389/tcp 10.100.35.113 on port 443/tcp 10.100.35.104 on port 443/tcp 10.100.35.89 on port 3389/tcp 10.100.35.87 on port 443/tcp 10.100.35.73 on port 3001/tcp 192.168.2.22 on port 3389/tcp 192.168.2.18 on port 54433/tcp 192.168.2.8 on port 1433/tcp 192.168.2.8 on port 2002/tcp 192.168.2.6 on port 3389/tcp 10.100.35.119 on port 3389/tcp 10.100.35.101 on port 443/tcp 10.100.35.51 on port 443/tcp 10.100.35.50 on port 443/tcp 10.100.34.85 on port 3389/tcp 10.100.33.61 on port 3389/tcp 10.100.33.59 on port 3389/tcp 10.100.33.54 on port 3389/tcp 10.100.33.52 on port 443/tcp 10.100.32.65 on port 3389/tcp 10.100.31.82 on port 443/tcp 10.100.31.81 on port 443/tcp 10.100.31.69 on port 443/tcp 10.100.31.69 on port 5061/tcp 10.100.31.60 on port 443/tcp 10.100.31.54 on port 443/tcp 10.100.31.52 on port 443/tcp 10.100.20.200 on port 1433/tcp 10.100.20.33 (lt186) on port 3389/tcp 10.100.7.210 on port 3389/tcp 10.100.7.210 on port 3071/tcp 10.100.7.201 on port 3389/tcp 10.100.7.135 on port 3389/tcp

	10.100.7.131 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.119 on port 1433/tcp 10.100.7.118 on port 3389/tcp 10.100.7.116 on port 1433/tcp 10.100.7.115 on port 3389/tcp 10.100.7.111 on port 3071/tcp 10.100.7.110 on port 3389/tcp 10.100.7.96 on port 9080/tcp 10.100.7.95 (IT09-5Z5KN53) on port 9080/tcp 10.100.7.88 (URSIOSSVR01) on port 3389/tcp 10.100.7.86 (HIST-01A) on port 1433/tcp 10.100.7.85 (MPM) on port 1433/tcp 10.100.7.84 (HMI1) on port 3389/tcp 10.100.7.82 (TESTPC06) on port 3389/tcp 10.100.7.78 (OSSEM3_RIUHMI01) on port 3389/tcp 10.100.7.75 (IT03-5D3BVV1) on port 3389/tcp 10.100.7.74 on port 443/tcp 10.100.7.73 (VSS-01A) on port 1433/tcp 10.100.7.72 (DESKTOP-KOCHTQC) on port 3389/tcp 10.100.7.71 (VSS-01B) on port 1433/tcp 10.100.7.69 on port 443/tcp 10.100.7.66 (URSIOSSVR02) on port 3389/tcp 10.100.7.62 (OSSEM2_RIOHMI01) on port 3389/tcp 10.100.7.53 (URSHISTSVR01) on port 1433/tcp 10.100.7.53 (URSHISTSVR01) on port 3389/tcp 10.100.7.51 (it03-8ddvdv1) on port 3389/tcp 10.100.6.90 (IT01-FT0Y4Y2) on port 3389/tcp 10.100.6.81 (IT01-CX9WNW1) on port 3389/tcp 10.100.6.65 (IT01-B11Y4Y2) on port 3389/tcp 10.100.6.20 on port 443/tcp 10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp 10.100.5.68 (IT02-2SD5Y2) on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp 10.100.5.60 (IT08-DF9HLW2) on port 3389/tcp 10.100.5.58 on port 443/tcp 10.100.3.64 (IT01-4P775Y2) on port 3389/tcp 10.100.3.52 (IT10-CM1V8Y1) on port 3389/tcp 10.100.3.51 (IT03-4M7MM32) on port 3389/tcp 10.100.2.93 (IT10-DHVDT13) on port 3389/tcp 10.100.2.70 (IT09-6GRJN53) on port 443/tcp 10.100.2.60 on port 9080/tcp 10.100.2.58 on port 9080/tcp 10.100.2.57 on port 9080/tcp 10.100.2.56 on port 9080/tcp 10.100.2.54 (IT09-1KBKLR2) on port 3389/tcp 10.100.2.53 (it05-100625) on port 3389/tcp 10.100.2.53 (it05-100625) on port 8191/tcp 10.100.2.53 (it05-100625) on port 8089/tcp 10.100.2.49 (IT09-H42HYV1) on port 3389/tcp 10.100.2.49 (IT09-H42HYV1) on port 443/tcp 10.100.2.45 on port 8443/tcp 10.100.2.45 on port 443/tcp 10.100.1.151 on port 443/tcp 10.100.1.150 on port 443/tcp 10.100.1.99 (IT10-BVMFJX2) on port 3389/tcp 10.100.2.81 (WindUtilWS) on port 3389/tcp 10.100.1.80 on port 8009/tcp 10.100.1.76 (IT10-F8BP2R1) on port 3389/tcp
Additional Output	The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities : |-Subject : CN=shipping-imac.local

SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

Severity	
Description	The remote service encrypts traffic using TLS / SSL but allows a client to insecurely renegotiate the connection after the initial handshake. An unauthenticated, remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer. The remote service allows insecure renegotiation of TLS / SSL connections.
CVSS	5.8 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)
Recommendation	Contact the vendor for specific patch information.
References	http://www.ietf.org/mail-archive/web/tls/current/msg03948.html http://www.g-sec.lu/practicaltls.pdf https://tools.ietf.org/html/rfc5746
Affected Nodes	192.168.2.64 on port 443/tcp 192.168.2.63 on port 443/tcp 192.168.2.61 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.59 on port 443/tcp

Additional Output	`TLSv1 supports insecure renegotiation.`
	
	`SSLv3 supports insecure renegotiation.`

SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Severity	
Description	The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections. As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service. The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism. This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability. It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS3	6.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N)
Recommendation	Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.
References	https://www.imperialviolet.org/2014/10/14/poodle.html https://www.openssl.org/~bodo/ssl-poodle.pdf https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00
Affected Nodes	192.168.2.64 on port 443/tcp 192.168.2.63 on port 443/tcp 192.168.2.62 on port 443/tcp 192.168.2.61 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.59 on port 443/tcp 192.168.2.18 on port 54433/tcp

	192.168.2.3 on port 443/tcp 192.168.2.19 on port 443/tcp 192.168.2.5 on port 902/tcp 192.168.2.5 on port 5989/tcp 192.168.2.5 on port 443/tcp 192.168.2.3 on port 902/tcp 192.168.2.3 on port 5989/tcp 10.100.20.200 on port 1433/tcp 10.100.7.119 on port 1433/tcp 10.100.7.116 on port 1433/tcp 10.100.7.210 on port 3071/tcp 10.100.7.111 on port 3071/tcp 10.100.7.53 (URSHISTSVR01) on port 1433/tcp 10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp 10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp

Additional Output	`vPenTest Partner determined that the remote server supports SSLv3 with at least one CBC cipher suite, indicating that this server is vulnerable.`
	
	`It appears that TLSv1 or newer is supported on the server. However, the Fallback SCSV mechanism is not supported, allowing connections to be "rolled back" to SSLv3.`

Terminal Services Doesn't Use Network Level Authentication (NLA) Only	
Severity	
Description	The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established. The remote Terminal Services doesn't use Network Level Authentication only.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS3	4.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N)
Recommendation	Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.
References	https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11) http://www.nessus.org/u?e2628096
Affected Nodes	192.168.2.71 on port 3389/tcp 192.168.2.19 on port 3389/tcp 10.100.35.119 on port 3389/tcp 10.100.35.89 on port 3389/tcp 10.100.34.85 on port 3389/tcp 10.100.33.61 on port 3389/tcp 10.100.33.59 on port 3389/tcp 10.100.33.54 on port 3389/tcp 10.100.32.65 on port 3389/tcp 10.100.20.33 (lt186) on port 3389/tcp 10.100.7.210 on port 3389/tcp 10.100.7.201 on port 3389/tcp 10.100.7.135 on port 3389/tcp 10.100.7.131 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.115 on port 3389/tcp 10.100.7.84 (HMI1) on port 3389/tcp 10.100.7.78 (OSSEM3_RIUHMI01) on port 3389/tcp 10.100.7.72 (DESKTOP-KOCHTQC) on port 3389/tcp 10.100.7.62 (OSSEM2_RIOHMI01) on port 3389/tcp 10.100.6.90 (IT01-FT0Y4Y2) on port 3389/tcp 10.100.6.65 (IT01-B11Y4Y2) on port 3389/tcp 10.100.5.68 (IT02-2SD5Y2) on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp

	10.100.5.60 (IT08-DF9HLW2) on port 3389/tcp 10.100.3.64 (IT01-4P775Y2) on port 3389/tcp 10.100.3.52 (IT10-CM1V8Y1) on port 3389/tcp 10.100.2.93 (IT10-DHVDT13) on port 3389/tcp 10.100.2.81 (WindUtilWS) on port 3389/tcp 10.100.2.53 (it05-100625) on port 3389/tcp 10.100.2.49 (IT09-H42HYV1) on port 3389/tcp 10.100.1.99 (IT10-BVMFJX2) on port 3389/tcp 10.100.1.76 (IT10-F8BP2R1) on port 3389/tcp
Additional Output	`vPenTest Partner was able to negotiate non-NLA (Network Level Authentication) security.`

Terminal Services Encryption Level is Medium or Low	
Severity	
Description	The remote Terminal Services service is not configured to use strong cryptography. Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes. The remote host is using weak cryptography.
CVSS	4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
Recommendation	Change RDP encryption level to one of : 3. High 4. FIPS Compliant
References	n/a
Affected Nodes	192.168.2.71 on port 3389/tcp 10.100.7.210 on port 3389/tcp 10.100.7.136 on port 3389/tcp 10.100.7.135 on port 3389/tcp 10.100.7.131 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.115 on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp 10.100.2.49 (IT09-H42HYV1) on port 3389/tcp

Additional Output	`The terminal services encryption level is set to :`
	
	`2. Medium`

Unencrypted Telnet Server	
Severity	
Description	The remote host is running a Telnet server over an unencrypted channel. Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server. SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session. The remote Telnet server transmits traffic in cleartext.
CVSS	5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)
CVSS3	6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
Recommendation	Disable the Telnet service and use SSH instead.
References	n/a

Affected Nodes	192.168.2.2 on port 60000/tcp 10.100.35.5 on port 23/tcp 10.100.34.15 on port 23/tcp 10.100.34.5 on port 23/tcp 10.100.33.15 on port 23/tcp 10.100.33.5 on port 23/tcp 10.100.32.5 on port 23/tcp 10.100.32.15 on port 23/tcp 10.100.31.5 on port 23/tcp 10.100.7.74 on port 23/tcp 10.100.7.63 on port 23/tcp 10.100.7.64 on port 23/tcp 10.100.7.5 on port 23/tcp 10.100.6.25 on port 9999/tcp 10.100.6.5 on port 23/tcp 10.100.5.58 on port 23/tcp 10.100.5.25 on port 23/tcp 10.100.5.5 on port 23/tcp 10.100.4.5 on port 23/tcp 10.100.6.26 on port 9999/tcp 10.100.3.25 on port 23/tcp 10.100.3.5 on port 23/tcp 10.100.2.5 on port 23/tcp 10.100.1.25 on port 23/tcp 10.100.1.5 on port 23/tcp

Additional Output	`vPenTest Partner collected the following banner from the remote Telnet server :`
	
	`------------------------------ snip ------------------------------`
	
	`>`
	`------------------------------ snip ------------------------------`

VMware ESXi Multiple DoS (VMSA-2014-0008)

Severity	
Description	The remote ESXi host is affected by multiple denial of service vulnerabilities in the glibc library : - A buffer overflow condition exists in the extend_buffers() function in file posix/regexec.c due to improper validation of user-supplied input when handling multibyte characters in a regular expression. An unauthenticated, remote attacker can exploit this, via a crafted regular expression, to corrupt the memory, resulting in a denial of service. (CVE-2013-0242) - A stack-based buffer overflow condition exists in the getaddrinfo() function in file posix/getaddrinfo.c due to improper validation of user-supplied input during the handling of domain conversion results. An unauthenticated, remote attacker can exploit this to cause a denial of service by using a crafted host name or IP address that triggers a large number of domain conversion results. (CVE-2013-1914) The remote VMware ESXi host is missing a security-related patch.
CVSS	5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)
Recommendation	Apply the appropriate patch according to the vendor advisory that pertains to ESXi version 5.0 / 5.1 / 5.5.
References	https://www.vmware.com/security/advisories/VMSA-2014-0008 http://lists.vmware.com/pipermail/security-announce/2014/000282.html
Affected Nodes	192.168.2.5 on port 443/tcp 192.168.2.3 on port 443/tcp

Additional Output	`Version         : ESXi 5.1`
	`  Installed build : 2000251`
	`  Fixed build     : 2323236`

VMware ESXi Multiple Vulnerabilities (VMSA-2014-0012)

Severity	
Description	The remote VMware ESXi host is affected by multiple vulnerabilities : - Multiple denial of service vulnerabilities exist in Python function _read_status() in library httplib and in function readline() in libraries smtplib, ftplib, nntplib, imaplib, and poplib. A remote attacker can exploit these vulnerabilities to crash the module. (CVE-2013-1752) - A out-of-bounds read error exists in file parser.c in library libxml2 due to a failure to properly check the XML_PARSER_EOF state. An unauthenticated, remote attacker can exploit this, via a crafted document that abruptly ends, to cause a denial of service. (CVE-2013-2877) - A spoofing vulnerability exists in the Python SSL module in the ssl.match_hostname() function due to improper handling of the NULL character ('\0') in a domain name in the Subject Alternative Name field of an X.509 certificate. A man-in-the-middle attacker can exploit this, via a crafted certificate issued by a legitimate certification authority, to spoof arbitrary SSL servers. (CVE-2013-4238) - cURL and libcurl are affected by a flaw related to the re-use of NTLM connections whenever more than one authentication method is enabled. An unauthenticated, remote attacker can exploit this, via a crafted request, to connect and impersonate other users. (CVE-2014-0015) - The default configuration in cURL and libcurl reuses the SCP, SFTP, POP3, POP3S, IMAP, IMAPS, SMTP, SMTPS, LDAP, and LDAPS connections. An unauthenticated, remote attacker can exploit this, via a crafted request, to connect and impersonate other users. (CVE-2014-0138) - A flaw exists in the xmlParserHandlePEReference() function in file parser.c in libxml2 due to loading external entities regardless of entity substitution or validation being enabled. An unauthenticated, remote attacker can exploit this, via a crafted XML document, to exhaust resources, resulting in a denial of service. (CVE-2014-0191) The remote VMware ESXi host is missing a security-related patch.
CVSS	6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)
Recommendation	Apply the appropriate patch according to the vendor advisory that pertains to ESXi version 5.0 / 5.1 / 5.5.
References	https://www.vmware.com/security/advisories/VMSA-2014-0012 http://lists.vmware.com/pipermail/security-announce/2015/000287.html
Affected Nodes	192.168.2.5 on port 443/tcp 192.168.2.3 on port 443/tcp

Additional Output	`Version : ESXi 5.1`
	`Installed build : 2000251`
	`Fixed build : 2323236`

DHCP Server Detection

Severity	
Description	This script contacts the remote DHCP server (if any) and attempts to retrieve information about the network layout. Some DHCP servers provide sensitive information such as the NIS domain name, or network layout information such as the list of the network web servers, and so on. It does not demonstrate any vulnerability, but a local attacker may use DHCP to become intimately familiar with the associated network. The remote DHCP server may expose information about the associated network.
CVSS	3.3 (CVSS2#AV:A/AC:L/Au:N/C:P/I:N/A:N)
Recommendation	Apply filtering to keep this information off the network and remove any options that are not in use.
References	n/a
Affected Nodes	10.100.2.5 on port 67/udp

Additional Output	vPenTest Partner gathered the following information from the remote DHCP server : Master DHCP server of this network : 192.168.204.139 IP address the DHCP server would attribute us : 10.100.2.51 Netmask : 255.255.255.0 DHCP server(s) identifier : 192.168.204.52 Router : 10.100.2.5 Domain name server(s) : 192.168.204.60 , 192.168.204.66 Domain name : w-industries.com

OpenSSL 1.0.2 < 1.0.2t Multiple Vulnerabilities

Severity	
Description	The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by multiple vulnerabilities : - Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by this issue. (CVE-2019-1547) - OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verification in TLS. This directory is most commonly referred to as OPENSSLDIR, and is configurable with the --prefix / --openssldir configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the mingw configuration targets assume that resulting programs and libraries are installed in a Unix-like environment and the default prefix for program installation as well as for OPENSSLDIR should be '/usr/local'. However, mingw programs are Windows programs, and as such, find themselves looking at sub-directories of 'C:/usr/local', which may be world writable, which enables untrusted users to modify OpenSSL's default configuration, insert CA certificates, modify (or even replace) existing engine modules, etc. For OpenSSL 1.0.2, '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and Windows targets, including Visual C builds. However, some build instructions for the diverse Windows targets on 1.0.2 encourage you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. (CVE-2019-1552) Note that vPenTest Partner has not tested for these issues but has instead relied only on the application's self-reported version number. The remote service is affected by multiple vulnerabilities.
CVSS	1.9 (CVSS2#AV:L/AC:M/Au:N/C:N/I:P/A:N)
CVSS3	3.3 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N)
Recommendation	Upgrade to OpenSSL version 1.0.2t or later.
References	http://www.nessus.org/u?27ebc9b1 https://www.openssl.org/news/secadv/20190910.txt https://www.openssl.org/news/secadv/20190730.txt
Affected Nodes	10.100.6.87 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.6.20 on port 443/tcp
Additional Output	Banner : Apache/2.4.20 (Unix) OpenSSL/1.0.2j Reported version : 1.0.2j Fixed version : 1.0.2t

SSH Server CBC Mode Ciphers Enabled

Severity	

Description	The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext. Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions. The SSH server is configured to use Cipher Block Chaining.
CVSS	2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
Recommendation	Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.
References	n/a
Affected Nodes	10.100.34.84 on port 22/tcp 10.100.34.81 on port 22/tcp 10.100.34.80 on port 22/tcp 10.100.34.77 on port 22/tcp 10.100.34.74 on port 22/tcp 10.100.34.73 on port 22/tcp 10.100.34.71 on port 22/tcp 10.100.34.70 on port 22/tcp 10.100.34.69 on port 22/tcp 10.100.34.68 on port 22/tcp 10.100.34.65 on port 22/tcp 10.100.34.64 on port 22/tcp 10.100.34.61 on port 22/tcp 10.100.34.60 on port 22/tcp 10.100.34.59 on port 22/tcp 10.100.34.58 on port 22/tcp 10.100.34.56 on port 22/tcp 10.100.34.55 on port 22/tcp 10.100.34.54 on port 22/tcp 10.100.34.53 on port 22/tcp 10.100.34.52 on port 22/tcp 10.100.34.51 on port 22/tcp 10.100.34.50 on port 22/tcp 10.100.33.60 on port 22/tcp 10.100.33.57 on port 22/tcp 10.100.34.79 on port 22/tcp 10.100.34.78 on port 22/tcp 10.100.34.76 on port 22/tcp 10.100.34.75 on port 22/tcp 10.100.34.72 on port 22/tcp 10.100.34.67 on port 22/tcp 10.100.34.66 on port 22/tcp 10.100.34.63 on port 22/tcp 10.100.34.62 on port 22/tcp 10.100.34.57 on port 22/tcp 10.100.33.55 on port 22/tcp 10.100.33.50 on port 22/tcp 10.100.32.69 on port 22/tcp 10.100.32.59 on port 22/tcp 10.100.32.57 on port 22/tcp 10.100.32.56 on port 22/tcp 10.100.32.53 on port 22/tcp 10.100.32.52 on port 22/tcp 10.100.32.51 on port 22/tcp 10.100.32.50 on port 22/tcp 10.100.31.80 on port 22/tcp 10.100.31.77 on port 22/tcp 10.100.31.75 on port 22/tcp 10.100.31.73 on port 22/tcp 10.100.31.71 on port 22/tcp 10.100.31.67 on port 22/tcp 10.100.32.62 on port 22/tcp 10.100.32.61 on port 22/tcp 10.100.32.58 on port 22/tcp 10.100.32.55 on port 22/tcp

	10.100.32.54 on port 22/tcp 10.100.31.58 on port 22/tcp 10.100.31.56 on port 22/tcp 10.100.31.55 on port 22/tcp 10.100.31.53 on port 22/tcp 10.100.31.51 on port 22/tcp 10.100.7.98 on port 2222/tcp 10.100.7.98 on port 22/tcp 10.100.7.97 on port 2222/tcp 10.100.7.97 on port 22/tcp 10.100.31.50 on port 22/tcp 10.100.7.74 on port 22/tcp 10.100.5.53 on port 22/tcp 10.100.5.52 on port 22/tcp

Additional Output	`The following client-to-server Cipher Block Chaining (CBC) algorithms are supported :`
	
	`3des-cbc`
	`aes128-cbc`
	`aes256-cbc`
	
	`The following server-to-client Cipher Block Chaining (CBC) algorithms are supported :`
	
	`3des-cbc`
	`aes128-cbc`
	`aes256-cbc`

SSH Weak MAC Algorithms Enabled	
Severity	
Description	The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak. Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions. The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.
CVSS	2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
Recommendation	Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.
References	n/a
Affected Nodes	10.100.34.84 on port 22/tcp 10.100.34.80 on port 22/tcp 10.100.34.79 on port 22/tcp 10.100.34.78 on port 22/tcp 10.100.34.76 on port 22/tcp 10.100.34.73 on port 22/tcp 10.100.34.67 on port 22/tcp 10.100.34.66 on port 22/tcp 10.100.34.65 on port 22/tcp 10.100.34.64 on port 22/tcp 10.100.34.62 on port 22/tcp 10.100.34.60 on port 22/tcp 10.100.34.59 on port 22/tcp 10.100.34.58 on port 22/tcp 10.100.34.57 on port 22/tcp 10.100.34.55 on port 22/tcp 10.100.34.53 on port 22/tcp 10.100.34.52 on port 22/tcp 10.100.34.51 on port 22/tcp 10.100.34.50 on port 22/tcp 10.100.33.60 on port 22/tcp 10.100.34.81 on port 22/tcp 10.100.34.77 on port 22/tcp

	10.100.34.75 on port 22/tcp 10.100.34.74 on port 22/tcp 10.100.34.72 on port 22/tcp 10.100.34.71 on port 22/tcp 10.100.34.70 on port 22/tcp 10.100.34.69 on port 22/tcp 10.100.34.68 on port 22/tcp 10.100.34.63 on port 22/tcp 10.100.34.61 on port 22/tcp 10.100.34.56 on port 22/tcp 10.100.34.54 on port 22/tcp 10.100.33.57 on port 22/tcp 10.100.33.55 on port 22/tcp 10.100.33.50 on port 22/tcp 10.100.32.69 on port 22/tcp 10.100.32.62 on port 22/tcp 10.100.32.61 on port 22/tcp 10.100.32.59 on port 22/tcp 10.100.32.58 on port 22/tcp 10.100.32.56 on port 22/tcp 10.100.32.55 on port 22/tcp 10.100.32.54 on port 22/tcp 10.100.32.53 on port 22/tcp 10.100.31.80 on port 22/tcp 10.100.31.77 on port 22/tcp 10.100.31.75 on port 22/tcp 10.100.31.73 on port 22/tcp 10.100.31.71 on port 22/tcp 10.100.31.58 on port 22/tcp 10.100.32.57 on port 22/tcp 10.100.32.52 on port 22/tcp 10.100.32.51 on port 22/tcp 10.100.32.50 on port 22/tcp 10.100.31.67 on port 22/tcp 10.100.31.56 on port 22/tcp 10.100.31.55 on port 22/tcp 10.100.31.53 on port 22/tcp 10.100.31.50 on port 22/tcp 10.100.7.98 on port 2222/tcp 10.100.7.97 on port 2222/tcp 10.100.31.51 on port 22/tcp 10.100.5.53 on port 22/tcp 10.100.5.52 on port 22/tcp 10.100.3.53 on port 22/tcp 10.100.1.96 on port 22/tcp

Additional Output	The following client-to-server Message Authentication Code (MAC) algorithms
	are supported :
	
	  hmac-sha1-96
	
	The following server-to-client Message Authentication Code (MAC) algorithms
	are supported :
	
	  hmac-sha1-96

SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Severity	
Description	The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext. The remote service supports the use of the RC4 cipher.

CVSS	2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
CVSS3	5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
Recommendation	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.
References	http://www.nessus.org/u?ac7327a0 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf
Affected Nodes	192.168.2.64 on port 443/tcp 192.168.2.61 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.59 on port 443/tcp 192.168.2.58 on port 443/tcp 192.168.2.58 on port 1883/tcp 192.168.2.56 on port 1883/tcp 192.168.2.56 on port 443/tcp 192.168.2.63 on port 443/tcp 192.168.2.62 on port 443/tcp 192.168.2.57 on port 1883/tcp 192.168.2.57 on port 443/tcp 192.168.2.55 on port 1883/tcp 192.168.2.55 on port 443/tcp 192.168.2.51 on port 443/tcp 192.168.2.8 on port 1433/tcp 192.168.2.6 on port 3389/tcp 10.100.35.104 on port 443/tcp 10.100.35.87 on port 443/tcp 10.100.35.73 on port 3001/tcp 192.168.2.19 on port 3389/tcp 192.168.2.19 on port 443/tcp 192.168.2.18 on port 54433/tcp 192.168.2.18 on port 3389/tcp 192.168.2.8 on port 3389/tcp 10.100.35.113 on port 443/tcp 10.100.35.101 on port 443/tcp 10.100.35.51 on port 443/tcp 10.100.34.80 on port 443/tcp 10.100.34.65 on port 443/tcp 10.100.7.210 on port 3389/tcp 10.100.7.135 on port 3389/tcp 10.100.7.131 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.119 on port 1433/tcp 10.100.7.115 on port 3389/tcp 10.100.7.111 on port 3071/tcp 10.100.7.110 on port 3389/tcp 10.100.7.210 on port 3071/tcp 10.100.7.88 (URSIOSSVR01) on port 3389/tcp 10.100.7.86 (HIST-01A) on port 1433/tcp 10.100.7.84 (HMI1) on port 3389/tcp 10.100.7.78 (OSSEM3_RIUHMI01) on port 3389/tcp 10.100.7.73 (VSS-01A) on port 1433/tcp 10.100.7.72 (DESKTOP-KOCHTQC) on port 3389/tcp 10.100.7.71 (VSS-01B) on port 1433/tcp 10.100.7.66 (URSIOSSVR02) on port 3389/tcp 10.100.7.62 (OSSEM2_RIOHMI01) on port 3389/tcp 10.100.7.53 (URSHISTSVR01) on port 1433/tcp 10.100.7.53 (URSHISTSVR01) on port 3389/tcp 10.100.7.51 (it03-8ddvdv1) on port 3389/tcp 10.100.7.85 (MPM) on port 1433/tcp 10.100.7.74 on port 443/tcp 10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp 10.100.5.58 on port 443/tcp
Additional Output	`List of RC4 cipher suites supported by the remote server :`

```
  High Strength Ciphers (>= 112-bit key)

    Name                        Code            KEX          Auth     Encryption            MAC
    ----------------------      ----------      ---          ----     --------------------  ---
    RC4-SHA                     0x00, 0x05      RSA          RSA      RC4(128)              SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	
Severity	
Description	The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections. The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.
CVSS	2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)
CVSS3	3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)
Recommendation	Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.
References	https://weakdh.org/
Affected Nodes	192.168.2.19 on port 3389/tcp 192.168.2.19 on port 443/tcp 192.168.2.18 on port 54433/tcp 192.168.2.18 on port 3389/tcp 192.168.2.8 on port 3389/tcp 192.168.2.6 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.51 (it03-8ddvdv1) on port 3389/tcp 10.100.7.88 (URSIOSSVR01) on port 3389/tcp 10.100.7.66 (URSIOSSVR02) on port 3389/tcp
Additional Output	

```
Vulnerable connection combinations :

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.0
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.1
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard
------------ snipped ------------
```

Terminal Services Encryption Level is not FIPS-140 Compliant	
Severity	
Description	The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant. The remote host is not FIPS-140 compliant.
CVSS	2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
Recommendation	Change RDP encryption level to : 4. FIPS Compliant
References	n/a
Affected Nodes	192.168.2.71 on port 3389/tcp 10.100.7.210 on port 3389/tcp 10.100.7.136 on port 3389/tcp 10.100.7.135 on port 3389/tcp 10.100.7.131 on port 3389/tcp 10.100.7.125 on port 3389/tcp 10.100.7.115 on port 3389/tcp 10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp 10.100.2.49 (IT09-H42HYV1) on port 3389/tcp

Additional Output	`The terminal services encryption level is set to :`
	
	`2. Medium (Client Compatible)`

Transport Layer Security (TLS) Protocol CRIME Vulnerability	
Severity	
Description	The remote service has one of two configurations that are known to be required for the CRIME attack : - SSL / TLS compression is enabled. - TLS advertises the SPDY protocol earlier than version 4. Note that vPenTest Partner did not attempt to launch the CRIME attack against the remote service. The remote service has a configuration that may make it vulnerable to the CRIME attack.
CVSS	2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
Recommendation	Disable compression and / or the SPDY service.
References	https://www.iacr.org/cryptodb/data/paper.php?pubkey=3091 https://discussions.nessus.org/thread/5546 http://www.nessus.org/u?c44d5826 https://bz.apache.org/bugzilla/show_bug.cgi?id=53219
Affected Nodes	192.168.2.5 on port 5989/tcp 192.168.2.3 on port 443/tcp 192.168.2.5 on port 443/tcp 192.168.2.3 on port 5989/tcp 10.100.2.53 (it05-100625) on port 8089/tcp

Additional Output	`The following configuration indicates that the remote service`
	`may be vulnerable to the CRIME attack :`
	
	`  - SSL / TLS compression is enabled.`

Apache Banner Linux Distribution Disclosure	
Severity	

Description	vPenTest Partner was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running. The name of the Linux distribution running on the remote host was found in the banner of the web server.
Recommendation	If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache. n/a
References	n/a
Affected Nodes	192.168.2.51 on port 0/tcp
Additional Output	`The Linux distribution detected was :` `- CentOS 7`

Apple iOS Lockdown Detection

Severity	
Description	The lockdown service, part of Apple iOS, was detected on the remote host. This service is used to communicate with iOS devices for several tasks (e.g., Wi-Fi sync). Note that this plugin will only work against devices that have ever had Wi-Fi sync enabled (iOS versions 5 and later).
Recommendation	n/a
References	n/a
Affected Nodes	10.100.20.173 on port 62078/tcp
Additional Output	`n/a`

Appweb HTTP Server Version

Severity	
Description	The remote host is running the Appweb HTTP Server, an open source web server. It was possible to read its version number from the banner. Note that 'Embedthis' used to be known as 'Mbedthis' and 'Appweb' used to be known as 'AppWeb'. It is possible to obtain the version number of the remote Appweb HTTP server.
Recommendation	n/a
References	https://www.embedthis.com/
Affected Nodes	192.168.2.17 on port 9998/tcp 192.168.2.17 on port 9997/tcp 192.168.2.17 on port 80/tcp 192.168.2.17 on port 443/tcp
Additional Output	`Version source    : Mbedthis-Appweb/2.4.0` `  Installed version : 2.4.0`

AXIS FTP Server Detection

Severity	
Description	vPenTest Partner was able to detect the FTP interface for an AXIS device on the remote host. The FTP interface for an AXIS device is listening on the remote host.
Recommendation	n/a
References	https://www.axis.com/en-us
Affected Nodes	10.100.7.150 on port 21/tcp

	10.100.6.87 on port 21/tcp 10.100.3.151 on port 21/tcp 10.100.3.150 on port 21/tcp
Additional Output	Path : / Version : 6.35.1.1 confidence : 70 date : 2016 model : P5624-E MkII type : PTZ Dome Network Camera

Backported Security Patch Detection (FTP)	
Severity	
Description	Security patches may have been 'backported' to the remote FTP server without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem. Security patches are backported.
Recommendation	n/a
References	https://access.redhat.com/security/updates/backporting/?sc_cid=3093
Affected Nodes	192.168.2.51 on port 21/tcp
Additional Output	Give vPenTest Partner credentials to perform local checks.

Backported Security Patch Detection (PHP)	
Severity	
Description	Security patches may have been 'backported' to the remote PHP install without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem. Security patches have been backported.
Recommendation	n/a
References	https://access.redhat.com/security/updates/backporting/?sc_cid=3093
Affected Nodes	192.168.2.51 on port 443/tcp 192.168.2.51 on port 80/tcp
Additional Output	Give vPenTest Partner credentials to perform local checks.

Backported Security Patch Detection (WWW)	
Severity	
Description	Security patches may have been 'backported' to the remote HTTP server without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem. Security patches are backported.
Recommendation	n/a
References	https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Affected Nodes	192.168.2.51 on port 443/tcp 192.168.2.51 on port 80/tcp
Additional Output	`Give vPenTest Partner credentials to perform local checks.`

Citrix Licensing Service Detection	
Severity	
Description	The remote host is running Citrix Licensing Service.
Recommendation	If this service is not needed, disable it or filter incoming traffic to this port.
References	n/a
Affected Nodes	10.100.7.135 on port 27000/tcp 10.100.7.125 on port 27000/tcp 10.100.7.115 on port 27000/tcp 10.100.7.84 (HMI1) on port 27000/tcp
Additional Output	`n/a`

COM+ Internet Services (CIS) Server Detection	
Severity	
Description	COM+ Internet Services are RPC over HTTP tunneling and require IIS to operate. CIS ports shouldn't be visible on internet but only behind a firewall. A COM+ Internet Services (CIS) server is listening on this port.
Recommendation	If you do not use this service, disable it with DCOMCNFG. Otherwise, limit access to this port.
References	http://www.nessus.org/u?d02f7e6e https://support.microsoft.com/en-us/support/kb/articles/q282/2/61.asp
Affected Nodes	192.168.2.19 on port 3388/tcp 192.168.2.18 on port 1031/tcp 192.168.2.6 on port 1031/tcp

Additional Output	`Server banner :`
	
	`ncacn_http/1.0`

DNS Server Version Detection	
Severity	
Description	vPenTest Partner was able to obtain version information by sending a special TXT record query to the remote host. Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file. vPenTest Partner was able to obtain version information on the remote DNS server.
Recommendation	n/a
References	n/a
Affected Nodes	10.100.35.113 on port 53/udp 10.100.35.104 on port 53/udp 10.100.35.87 on port 53/udp 10.100.35.51 on port 53/udp

Additional Output	`DNS server answer for "version.bind" (over UDP) :`
	
	`  dnsmasq-2.80`

Do not scan printers (AppSocket)	
Severity	
Description	The remote host appears to be a network printer or multi-function device that supports the AppSocket (also known as JetDirect) protocol. Such devices often react very poorly when scanned - some crash, others print a number of pages. To avoid problems, vPenTest Partner has marked the remote host as 'Dead' and will not scan it. The remote host appears to be a printer and will not be scanned.
Recommendation	If you are not concerned about such behavior, enable the 'Scan Network Printers' setting under the 'Do not scan fragile devices' advanced settings block and re-run the scan.
References	n/a
Affected Nodes	192.168.2.24 on port 0/tcp 192.168.2.30 on port 0/tcp 192.168.2.23 on port 0/tcp 10.100.6.86 on port 0/tcp 10.100.6.67 on port 0/tcp 10.100.6.40 on port 0/tcp 10.100.5.71 on port 0/tcp 10.100.5.69 on port 0/tcp 10.100.2.76 on port 0/tcp 10.100.2.67 on port 0/tcp 10.100.1.53 (npi6b6417) on port 0/tcp
Additional Output	`The remote host seems to be an AppSocket printer.`

Dropbox Software Detection (uncredentialed check)	
Severity	
Description	Dropbox is installed on the remote host. Dropbox is an application for storing and synchronizing files between computers, possibly outside the organization. There is a file synchronization application on the remote host.
Recommendation	Ensure that use of this software agrees with your organization's acceptable use and security policies.
References	https://www.dropbox.com/
Affected Nodes	10.100.2.54 (IT09-1KBKLR2) on port 17500/udp
Additional Output	`The remote DropBox server broadcasts the following data :` `{"version": [2, 0], "port": 17500, "host_int": 199553306503176084638198191901618823749, "displaynam e": "", "namespaces": [5013350352]}`

Enumerate IPv6 Interfaces via SSH	
Severity	
Description	vPenTest Partner was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials. vPenTest Partner was able to enumerate the IPv6 interfaces on the remote host.
Recommendation	Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.
References	n/a
Affected Nodes	10.100.2.51 on port 0/tcp

Additional Output	`The following IPv6 interfaces are set on the remote host :`
	
	`- fe80::a00:27ff:fe5e:3a3a (on interface enp0s17)`
	`- ::1 (on interface lo)`

EtherNet/IP CIP Device Identification	
Severity	
Description	This plugin executes an EtherNet/IP Common Industrial Protocol (CIP) request to obtain device identification information, revision, and serial number. Use an EtherNet/IP CIP request to obtain the device identification.
Recommendation	n/a
References	n/a
Affected Nodes	10.100.7.125 on port 44818/tcp 10.100.7.93 (OWS-01A) on port 44818/udp 10.100.7.93 (OWS-01A) on port 44818/tcp 10.100.3.63 on port 44818/udp 10.100.3.63 on port 44818/tcp

Additional Output	`The following EtherNet/IP CIP device was found :`
	
	`Vendor name : Rockwell Software, Inc.`
	`Device type : unknown (11)`
	`Device name : RSLinx Server`
	`Product : 1`
	`Revision : 1.1`
	`Serial : 781652157`

FTP Server Detection	
Severity	
Description	It is possible to obtain the banner of the remote FTP server by connecting to a remote port. An FTP server is listening on a remote port.
Recommendation	n/a
References	n/a
Affected Nodes	192.168.2.51 on port 21/tcp 192.168.2.17 on port 21/tcp 10.100.7.150 on port 21/tcp 10.100.7.98 on port 21/tcp 10.100.7.97 on port 21/tcp 10.100.6.87 on port 21/tcp 10.100.3.151 on port 21/tcp 10.100.3.150 on port 21/tcp

Additional Output	`The remote FTP banner is :`
	
	`220 (vsFTPd 3.0.2)`

Grandstream Phone Web Interface Detection	
Severity	
Description	vPenTest Partner was able to detect the web interface for a Grandstream phone on the remote host. The web interface for a Grandstream phone was detected on the remote host.
Recommendation	n/a
References	http://www.grandstream.com/
Affected Nodes	10.100.34.84 on port 80/tcp 10.100.34.81 on port 80/tcp 10.100.34.80 on port 443/tcp 10.100.34.78 on port 80/tcp

	10.100.34.77 on port 80/tcp 10.100.34.75 on port 80/tcp 10.100.34.74 on port 80/tcp 10.100.34.72 on port 80/tcp 10.100.34.71 on port 80/tcp 10.100.34.70 on port 80/tcp 10.100.34.69 on port 80/tcp 10.100.34.68 on port 80/tcp 10.100.34.67 on port 80/tcp 10.100.34.66 on port 80/tcp 10.100.34.65 on port 443/tcp 10.100.34.64 on port 80/tcp 10.100.34.63 on port 80/tcp 10.100.34.62 on port 80/tcp 10.100.34.61 on port 80/tcp 10.100.34.60 on port 80/tcp 10.100.34.59 on port 80/tcp 10.100.34.58 on port 80/tcp 10.100.34.57 on port 80/tcp 10.100.34.56 on port 80/tcp 10.100.34.55 on port 80/tcp 10.100.34.54 on port 80/tcp 10.100.34.53 on port 80/tcp 10.100.34.52 on port 80/tcp 10.100.34.51 on port 80/tcp 10.100.34.50 on port 80/tcp 10.100.33.60 on port 80/tcp 10.100.34.79 on port 80/tcp 10.100.34.76 on port 80/tcp 10.100.34.73 on port 80/tcp 10.100.33.57 on port 80/tcp 10.100.33.55 on port 80/tcp 10.100.33.50 on port 80/tcp 10.100.32.69 on port 80/tcp 10.100.32.62 on port 80/tcp 10.100.32.61 on port 80/tcp 10.100.32.59 on port 80/tcp 10.100.32.58 on port 80/tcp 10.100.32.57 on port 80/tcp 10.100.32.56 on port 80/tcp 10.100.32.55 on port 80/tcp 10.100.32.54 on port 80/tcp 10.100.32.53 on port 80/tcp 10.100.32.52 on port 80/tcp 10.100.32.51 on port 80/tcp 10.100.32.50 on port 80/tcp 10.100.31.80 on port 80/tcp 10.100.31.77 on port 80/tcp 10.100.31.75 on port 80/tcp 10.100.31.73 on port 80/tcp 10.100.31.71 on port 80/tcp 10.100.31.56 on port 80/tcp 10.100.31.55 on port 80/tcp 10.100.31.67 on port 80/tcp 10.100.31.58 on port 80/tcp 10.100.31.53 on port 80/tcp 10.100.31.51 on port 80/tcp 10.100.31.50 on port 80/tcp 10.100.5.53 on port 80/tcp 10.100.5.52 on port 80/tcp

Additional Output	`URL : http://10.100.34.84/`
	`Version : 1.0.3.6`
	`model : GRP2614`

LDAP Crafted Search Request Server Information Disclosure

Severity	

	
Description	By sending a search request with a filter set to 'objectClass=*', it is possible to extract information about the remote LDAP server. It is possible to discover information about the remote LDAP server.
Recommendation	n/a
References	n/a
Affected Nodes	192.168.2.18 on port 3268/tcp 192.168.2.18 on port 389/tcp 192.168.2.6 on port 3268/tcp 192.168.2.6 on port 389/tcp

Additional Output	[+]-namingContexts:
	  | DC=ad,DC=volta-us,DC=com
	  | CN=Configuration,DC=ad,DC=volta-us,DC=com
	  | CN=Schema,CN=Configuration,DC=ad,DC=volta-us,DC=com
	  | DC=ForestDnsZones,DC=ad,DC=volta-us,DC=com
	  | DC=DomainDnsZones,DC=ad,DC=volta-us,DC=com
	[+]-currentTime:
	  | 20210111222441.0Z
	[+]-subschemaSubentry:
	  | CN=Aggregate,CN=Schema,CN=Configuration,DC=ad,DC=volta-us,DC=com
	[+]-dsServiceName:
	  | CN=NTDS Settings,CN=VOL2K12DC02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuratio
	n,DC=ad,DC=volta-us,DC=com
	[+]-namingContexts:
	  | DC=ad,DC=volta-us,DC=com
	  | CN=Configuration,DC=ad,DC=volta-us,DC=com
	  | CN=Schema,CN=Configuration,DC=ad,DC=volta-us,DC=com
	  | DC=ForestDnsZones,DC=ad,DC=volta-us,DC=com
	  | DC=DomainDnsZones,DC=ad,DC=volta-us,DC=com
	[+]-defaultNamingContext:
	  | DC=ad,DC=volta-us,DC=com
	[+]-schemaNamingContext:
	  | CN=Schema,CN=Configuration,DC=ad,DC=volta-us,DC=com
	[+]-configurationNamingContext:
	  | CN=Configuration,DC=ad,DC=volta-
	------------ snipped ------------

lighttpd HTTP Server Detection	
Severity	
Description	vPenTest Partner was able to detect the lighttpd HTTP server by looking at the HTTP banner on the remote host. The lighttpd HTTP server was detected on the remote host.
Recommendation	n/a
References	https://www.lighttpd.net/
Affected Nodes	10.100.34.84 on port 80/tcp 10.100.34.81 on port 80/tcp 10.100.34.80 on port 443/tcp 10.100.34.80 on port 80/tcp 10.100.34.79 on port 80/tcp 10.100.34.78 on port 80/tcp 10.100.34.76 on port 80/tcp 10.100.34.75 on port 80/tcp 10.100.34.73 on port 80/tcp 10.100.34.72 on port 80/tcp 10.100.34.71 on port 80/tcp 10.100.34.70 on port 80/tcp 10.100.34.69 on port 80/tcp 10.100.34.68 on port 80/tcp 10.100.34.67 on port 80/tcp 10.100.34.66 on port 80/tcp

	10.100.34.65 on port 443/tcp 10.100.34.65 on port 80/tcp 10.100.34.64 on port 80/tcp 10.100.34.62 on port 80/tcp 10.100.34.61 on port 80/tcp 10.100.34.60 on port 80/tcp 10.100.34.59 on port 80/tcp 10.100.34.58 on port 80/tcp 10.100.34.57 on port 80/tcp 10.100.34.56 on port 80/tcp 10.100.34.54 on port 80/tcp 10.100.34.53 on port 80/tcp 10.100.34.52 on port 80/tcp 10.100.34.51 on port 80/tcp 10.100.34.50 on port 80/tcp 10.100.33.60 on port 80/tcp 10.100.33.57 on port 80/tcp 10.100.34.77 on port 80/tcp 10.100.34.74 on port 80/tcp 10.100.34.63 on port 80/tcp 10.100.34.55 on port 80/tcp 10.100.33.55 on port 80/tcp 10.100.33.50 on port 80/tcp 10.100.32.69 on port 80/tcp 10.100.32.62 on port 80/tcp 10.100.32.61 on port 80/tcp 10.100.32.59 on port 80/tcp 10.100.32.57 on port 80/tcp 10.100.32.56 on port 80/tcp 10.100.32.54 on port 80/tcp 10.100.32.53 on port 80/tcp 10.100.32.50 on port 80/tcp 10.100.31.80 on port 80/tcp 10.100.31.77 on port 80/tcp 10.100.31.75 on port 80/tcp 10.100.31.73 on port 80/tcp 10.100.31.71 on port 80/tcp 10.100.32.58 on port 80/tcp 10.100.32.55 on port 80/tcp 10.100.32.52 on port 80/tcp 10.100.32.51 on port 80/tcp 10.100.31.67 on port 80/tcp 10.100.31.58 on port 80/tcp 10.100.31.56 on port 80/tcp 10.100.31.55 on port 80/tcp 10.100.31.53 on port 80/tcp 10.100.31.51 on port 80/tcp 10.100.31.50 on port 80/tcp 10.100.5.53 on port 80/tcp 10.100.5.52 on port 80/tcp

Additional Output	`URL : http://10.100.34.84/`
	`Version : 1.4.52`
	`source : Server: lighttpd/1.4.52`

Link-Local Multicast Name Resolution (LLMNR) Detection	
Severity	
Description	The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions. The remote device supports LLMNR.
Recommendation	Make sure that use of this software conforms to your organization's acceptable use and security policies.
References	http://www.nessus.org/u?51eae65d http://technet.microsoft.com/en-us/library/bb878128.aspx

Affected Nodes	10.100.2.93 (IT10-DHVDT13) on port 5355/udp 10.100.2.83 (Training2) on port 5355/udp 10.100.2.82 (Training8) on port 5355/udp 10.100.2.81 (WindUtilWS) on port 5355/udp 10.100.2.70 (IT09-6GRJN53) on port 5355/udp 10.100.2.66 (IT10-34S1MQ1) on port 5355/udp 10.100.2.65 (IT09-JGYQ733) on port 5355/udp 10.100.2.64 (it10-g0wtsw1) on port 5355/udp 10.100.2.63 (WIN-NLN1IU84VKS) on port 5355/udp 10.100.2.59 (WIN-NLN1IU84VKS) on port 5355/udp 10.100.2.55 (Training3) on port 5355/udp 10.100.2.54 (IT09-1KBKLR2) on port 5355/udp 10.100.2.53 (it05-100625) on port 5355/udp 10.100.2.52 (WIN-NLN1IU84VKS) on port 5355/udp 10.100.2.49 (IT09-H42HYV1) on port 5355/udp
Additional Output	`According to LLMNR, the name of the remote host is 'IT10-DHVDT13'.`

mDNS Detection (Local Network)

Severity	
Description	The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running. This plugin attempts to discover mDNS used by hosts residing on the same network segment as vPenTest Partner. It is possible to obtain information about the remote host.
Recommendation	Filter incoming traffic to UDP port 5353, if desired.
References	n/a
Affected Nodes	10.100.2.66 (IT10-34S1MQ1) on port 5353/udp 10.100.2.49 (IT09-H42HYV1) on port 5353/udp 10.100.2.45 on port 5353/udp

Additional Output	`vPenTest Partner was able to extract the following information :`
	
	`  - mDNS hostname       : IT10-34S1MQ1.local.`

Microsoft SQL Server UDP Query Remote Version Disclosure

Severity	
Description	Microsoft SQL server has a function wherein remote users can query the database server for the version that is being run. The query takes place over the same UDP port that handles the mapping of multiple SQL server instances on the same machine. It is important to note that, after Version 8.00.194, Microsoft decided not to update this function. This means that the data returned by the SQL ping is inaccurate for newer releases of SQL Server. It is possible to determine the remote SQL server version.
Recommendation	If there is only a single SQL instance installed on the remote host, consider filter incoming traffic to this port.
References	n/a
Affected Nodes	192.168.2.8 on port 1434/udp 192.168.2.18 on port 1434/udp 10.100.7.125 on port 1434/udp 10.100.7.86 (HIST-01A) on port 1434/udp 10.100.7.85 (MPM) on port 1434/udp

Additional Output	`A 'ping' request returned the following information about the remote`
	`SQL instance :`
	
	`  ServerName   : VOL2K12DC02`

```
  InstanceName : SWPDM
  IsClustered  : No
  Version      : 12.0.4100.1
  tcp          : 54433
  np           : \\VOL2K12DC02\pipe\MSSQL$SWPDM\sql\query
```

Microsoft Windows SMB LanMan Pipe Server Listing Disclosure	
Severity	
Description	It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host. It is possible to obtain network information.
Recommendation	n/a
References	n/a
Affected Nodes	10.100.7.136 on port 445/tcp

Additional Output	`Here is the browse list of the remote host :`
	
	`HMI-1 ( os : 5.1 )`

MongoDB Detection	
Severity	
Description	A document-oriented database system is listening on the remote port. The remote host is running a database system.
Recommendation	n/a
References	https://www.mongodb.com/
Affected Nodes	10.100.2.53 (it05-100625) on port 8191/tcp
Additional Output	`Version     : 3.6.14` `  Git version : cbef87692475857c7ee6e764c8f5104b39c342a1`

MSRPC Service Detection	
Severity	
Description	The remote host is running a Windows RPC service. This service replies to the RPC Bind Request with a Bind Ack response. However it is not possible to determine the uuid of this service.
Recommendation	n/a
References	n/a
Affected Nodes	192.168.2.8 on port 135/tcp
Additional Output	`n/a`

NFS Server Superfluous	
Severity	
Description	The remote NFS server is not exporting any shares. Running an unused service unnecessarily increases the attack surface of the remote host.
CVSS	0.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:N)

CVSS3	0.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)
Recommendation	Disable this service.
References	n/a
Affected Nodes	192.168.2.6 on port 2049/tcp
Additional Output	`n/a`

NFS Share Export List

Severity	
Description	This plugin retrieves the list of NFS exported shares. The remote NFS server exports a list of shares.
Recommendation	Ensure each share is intended to be exported.
References	http://www.tldp.org/HOWTO/NFS-HOWTO/security.html
Affected Nodes	192.168.2.34 on port 2049/tcp

Additional Output	`Here is the export list of 192.168.2.34 :`
	
	`/hdd/ts fe80::226:73ff:fe0c:d610%cdce0`

ONVIF Device Services

Severity	
Description	vPenTest Partner was able to map the enabled ONVIF services on the remote device by sending a GetCapabilities SOAP request. The remote service responded to an ONVIF GetCapabilities request
Recommendation	Enable IP filtering if possible. Disable ONVIF if it isn't in use.
References	https://www.onvif.org/
Affected Nodes	10.100.33.20 on port 80/tcp 10.100.7.150 on port 80/tcp 10.100.6.87 on port 80/tcp 10.100.3.151 on port 80/tcp 10.100.6.20 on port 80/tcp 10.100.1.151 on port 80/tcp 10.100.1.150 on port 80/tcp

Additional Output	`The ONVIF server on port 80 supports these services:`
	
	`http://www.onvif.org/ver10/device/wsdl => http://10.100.33.20/onvif/device_service`
	`http://www.onvif.org/ver10/events/wsdl => http://10.100.33.20/onvif/services`
	`http://www.onvif.org/ver20/ptz/wsdl => http://10.100.33.20/onvif/services`
	`http://www.onvif.org/ver10/recording/wsdl => http://10.100.33.20/onvif/services`
	`http://www.onvif.org/ver10/replay/wsdl => http://10.100.33.20/onvif/services`
	`http://www.onvif.org/ver10/media/wsdl => http://10.100.33.20/onvif/services`
	`http://www.onvif.org/ver10/search/wsdl => http://10.100.33.20/onvif/services`

Open Network Video Interface Forum (ONVIF) Protocol Detection

Severity	
Description	The remote device answered a NetworkVideoTransmitter WS-Discovery request. Therefore, it supports ONVIF. The remote device supports ONVIF
Recommendation	Filter access to this port if desired.
References	https://www.onvif.org/

Affected Nodes	192.168.2.65 on port 3702/udp 10.100.33.20 on port 3702/udp 10.100.7.150 on port 3702/udp 10.100.6.87 on port 3702/udp 10.100.6.20 on port 3702/udp 10.100.3.151 on port 3702/udp 10.100.3.150 on port 3702/udp 10.100.1.151 on port 3702/udp 10.100.1.150 on port 3702/udp

Additional Output	`The ONVIF service listening on UDP port 3702 advertises`
	`the following information:`
	
	`Endpoint: http://192.168.2.65:85/onvif/device_service`
	`Name: Volta IVI03246`
	`Hardware: DS-9616NI-ST`

Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	
Severity	
Description	The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues. The remote Windows host supports the SMBv1 protocol.
Recommendation	Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.
References	https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/ https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and http://www.nessus.org/u?8dcab5e4 http://www.nessus.org/u?234f8ef8 http://www.nessus.org/u?4c7e0cf3
Affected Nodes	192.168.2.78 on port 445/tcp 192.168.2.8 on port 445/tcp 10.100.20.200 on port 445/tcp 10.100.7.210 on port 445/tcp 10.100.7.136 on port 445/tcp 10.100.7.135 on port 445/tcp 10.100.7.131 on port 445/tcp 10.100.7.125 on port 445/tcp 10.100.7.119 on port 445/tcp 10.100.7.115 on port 445/tcp 10.100.7.111 on port 445/tcp 10.100.7.110 on port 445/tcp 10.100.7.101 (SmartTool-TMP) on port 445/tcp 10.100.7.90 (HMI-01B) on port 445/tcp 10.100.7.88 (URSIOSSVR01) on port 445/tcp 10.100.7.87 (SmartTool) on port 445/tcp 10.100.7.86 (HIST-01A) on port 445/tcp 10.100.7.85 (MPM) on port 445/tcp 10.100.7.84 (HMI1) on port 445/tcp 10.100.7.78 (OSSEM3_RIUHMI01) on port 445/tcp 10.100.7.77 (HMI-01A) on port 445/tcp 10.100.7.73 (VSS-01A) on port 445/tcp 10.100.7.72 (DESKTOP-KOCHTQC) on port 445/tcp 10.100.7.71 (VSS-01B) on port 445/tcp 10.100.7.70 (EWS-01) on port 445/tcp 10.100.7.66 (URSIOSSVR02) on port 445/tcp 10.100.7.62 (OSSEM2_RIOHMI01) on port 445/tcp 10.100.7.53 (URSHISTSVR01) on port 445/tcp

	10.100.7.51 (it03-8ddvdv1) on port 445/tcp 10.100.6.81 (IT01-CX9WNW1) on port 445/tcp 10.100.6.80 (IT01-486J8V1-Wiring-PC) on port 445/tcp 10.100.5.64 (CONMSAUTHMI601) on port 445/tcp 10.100.5.59 (IT06-G8F8HF1) on port 445/tcp 10.100.2.64 (it10-g0wtsw1) on port 445/tcp 10.100.2.63 (WIN-NLN1IU84VKS) on port 445/tcp 10.100.2.59 (WIN-NLN1IU84VKS) on port 445/tcp 10.100.2.52 (WIN-NLN1IU84VKS) on port 445/tcp
Additional Output	`The remote host supports SMBv1.`

Service Detection: 3 ASCII Digit Code Responses

Severity	
Description	This plugin is a complement of find_service1.nasl. It attempts to identify services that return 3 ASCII digits codes (ie: FTP, SMTP, NNTP, ...) This plugin performs service detection.
Recommendation	n/a
References	n/a
Affected Nodes	10.100.7.150 on port 21/tcp 10.100.6.87 on port 21/tcp 10.100.3.151 on port 21/tcp 10.100.3.150 on port 21/tcp
Additional Output	`An FTP server is running on this port`

Session Initiation Protocol Detection

Severity	
Description	The remote system is running software that speaks the Session Initiation Protocol (SIP). SIP is a messaging protocol to initiate communication sessions between systems. It is a protocol used mostly in IP Telephony networks / systems to setup, control, and teardown sessions between two or more systems. The remote system is a SIP signaling device.
Recommendation	If possible, filter incoming connections to the port so that it is used only by trusted sources.
References	https://en.wikipedia.org/wiki/Session_Initiation_Protocol
Affected Nodes	10.100.31.66 on port 5060/tcp 10.100.31.65 on port 5060/udp 10.100.31.64 on port 5060/tcp 10.100.31.60 on port 5060/tcp 10.100.31.60 on port 5060/udp 10.100.31.69 on port 5061/tcp 10.100.31.69 on port 5060/tcp 10.100.31.69 on port 5060/udp 10.100.31.65 on port 5060/tcp 10.100.31.64 on port 5060/udp 10.100.3.57 on port 5060/tcp 10.100.3.57 on port 5060/udp 10.100.1.74 on port 5060/tcp 10.100.1.74 on port 5060/udp

Additional Output	`The remote service was identified as :`
	
	`  AXIS C1310-E Network Horn Speaker`
	
	`It supports the following options :`
	
	`  PRACK, INVITE, ACK, BYE, CANCEL, UPDATE, INFO, SUBSCRIBE, NOTIFY, REFER, MESSAGE, OPTIONS`

Splunk Management API Detection	
Severity	
Description	The remote web server is an instance of the Splunk management API. Splunk is a search, monitoring, and reporting tool for system administrators. An infrastructure monitoring tool is running on the remote host.
Recommendation	Limit incoming traffic to this port if desired.
References	https://www.splunk.com/en_us/software.html http://dev.splunk.com/restapi http://www.nessus.org/u?3aa0f4e2 https://www.splunk.com/en_us/download/universal-forwarder.html
Affected Nodes	10.100.2.53 (it05-100625) on port 8089/tcp

Additional Output	`URL : https://10.100.2.53:8089/`
	`Version : unknown`
	`Management API : 1`

Splunk Web Detection	
Severity	
Description	The web interface for Splunk is running on the remote host. Splunk is a search, monitoring, and reporting tool for system administrators. An infrastructure monitoring tool is running on the remote host.
Recommendation	n/a
References	https://www.splunk.com/en_us/software.html
Affected Nodes	10.100.2.53 (it05-100625) on port 8000/tcp

Additional Output	`URL : http://10.100.2.53:8000/`
	`Version : unknown`
	`License : Enterprise`
	`Web interface : 1`

SSL Certificate Signed Using SHA-1 Algorithm	
Severity	
Description	The remote service uses an SSL certificate chain that has been signed with SHA-1, a cryptographically weak hashing algorithm. This signature algorithm is known to be vulnerable to collision attacks. An attacker can potentially exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire on or between January 1, 2016 and December 31, 2016 as informational. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm. An SSL certificate in the certificate chain has been signed using the SHA-1 hashing algorithm.
Recommendation	n/a
References	https://blog.chromium.org/2014/09/gradually-sunsetting-sha-1.html https://tools.ietf.org/html/rfc3279
Affected Nodes	192.168.2.64 on port 443/tcp 192.168.2.63 on port 443/tcp 192.168.2.61 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.59 on port 443/tcp 192.168.2.58 on port 443/tcp

	192.168.2.56 on port 443/tcp 192.168.2.57 on port 443/tcp 192.168.2.55 on port 443/tcp
Additional Output	The following certificates were part of the certificate chain sent by the remote host, but contain hashes that are considered to be weak. |-Subject : C=US/ST=California/L=Sunnyvale/O=Ruckus Wireless, Inc. |-Signature Algorithm : SHA-1 With RSA Encryption |-Valid From : Dec 01 03:12:35 2006 GMT |-Valid To : Nov 28 03:12:35 2016 GMT

SSL Cipher Block Chaining Cipher Suites Supported

Severity	
Description	The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly. The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.
Recommendation	n/a
References	https://www.openssl.org/docs/manmaster/man1/ciphers.html http://www.nessus.org/u?cc4a822a https://www.openssl.org/~bodo/tls-cbc.txt
Affected Nodes	192.168.2.61 on port 443/tcp 192.168.2.60 on port 443/tcp 192.168.2.58 on port 443/tcp 192.168.2.58 on port 1883/tcp 192.168.2.56 on port 443/tcp 192.168.2.78 on port 3389/tcp 192.168.2.74 on port 3389/tcp 192.168.2.71 on port 3389/tcp 192.168.2.64 on port 443/tcp 192.168.2.63 on port 443/tcp 192.168.2.59 on port 443/tcp 192.168.2.57 on port 1883/tcp 192.168.2.57 on port 443/tcp 192.168.2.56 on port 1883/tcp 192.168.2.55 on port 1883/tcp 192.168.2.55 on port 443/tcp 192.168.2.51 on port 443/tcp 192.168.2.8 on port 1433/tcp 192.168.2.22 on port 3389/tcp 192.168.2.22 on port 443/tcp 192.168.2.19 on port 3389/tcp 192.168.2.19 on port 443/tcp 192.168.2.18 on port 54433/tcp 192.168.2.18 on port 3389/tcp 192.168.2.8 on port 3389/tcp 192.168.2.8 on port 2002/tcp 192.168.2.6 on port 3389/tcp 192.168.2.5 on port 902/tcp 192.168.2.5 on port 5989/tcp 192.168.2.5 on port 443/tcp 192.168.2.3 on port 902/tcp 192.168.2.3 on port 5989/tcp 192.168.2.3 on port 443/tcp 10.100.35.119 on port 3389/tcp 10.100.35.113 on port 443/tcp 10.100.35.104 on port 443/tcp 10.100.35.101 on port 443/tcp 10.100.35.89 on port 3389/tcp 10.100.35.87 on port 443/tcp 10.100.35.73 on port 3001/tcp

10.100.35.50 on port 443/tcp
10.100.34.80 on port 443/tcp
10.100.35.51 on port 443/tcp
10.100.34.85 on port 3389/tcp
10.100.34.65 on port 443/tcp
10.100.33.61 on port 3389/tcp
10.100.33.59 on port 3389/tcp
10.100.31.69 on port 443/tcp
10.100.33.54 on port 3389/tcp
10.100.33.52 on port 443/tcp
10.100.32.65 on port 3389/tcp
10.100.31.82 on port 443/tcp
10.100.31.81 on port 443/tcp
10.100.31.69 on port 5061/tcp
10.100.31.66 on port 443/tcp
10.100.31.65 on port 443/tcp
10.100.31.64 on port 443/tcp
10.100.31.60 on port 443/tcp
10.100.31.54 on port 443/tcp
10.100.31.52 on port 443/tcp
10.100.7.210 on port 3071/tcp
10.100.7.125 on port 3389/tcp
10.100.7.118 on port 3389/tcp
10.100.7.97 on port 443/tcp
10.100.20.200 on port 1433/tcp
10.100.20.33 (lt186) on port 3389/tcp
10.100.7.210 on port 3389/tcp
10.100.7.201 on port 3389/tcp
10.100.7.135 on port 3389/tcp
10.100.7.131 on port 3389/tcp
10.100.7.119 on port 1433/tcp
10.100.7.116 on port 1433/tcp
10.100.7.115 on port 3389/tcp
10.100.7.111 on port 3071/tcp
10.100.7.110 on port 3389/tcp
10.100.7.98 on port 443/tcp
10.100.7.96 on port 9080/tcp
10.100.7.96 on port 443/tcp
10.100.7.95 (IT09-5Z5KN53) on port 443/tcp
10.100.7.88 (URSIOSSVR01) on port 3389/tcp
10.100.7.86 (HIST-01A) on port 1433/tcp
10.100.7.85 (MPM) on port 1433/tcp
10.100.7.78 (OSSEM3_RIUHMI01) on port 3389/tcp
10.100.7.74 on port 443/tcp
10.100.7.73 (VSS-01A) on port 1433/tcp
10.100.7.71 (VSS-01B) on port 1433/tcp
10.100.7.62 (OSSEM2_RIOHMI01) on port 3389/tcp
10.100.7.51 (it03-8ddvdv1) on port 3389/tcp
10.100.7.95 (IT09-5Z5KN53) on port 9080/tcp
10.100.7.84 (HMI1) on port 3389/tcp
10.100.7.82 (TESTPC06) on port 3389/tcp
10.100.7.75 (IT03-5D3BVV1) on port 3389/tcp
10.100.7.72 (DESKTOP-KOCHTQC) on port 3389/tcp
10.100.7.69 on port 443/tcp
10.100.7.66 (URSIOSSVR02) on port 3389/tcp
10.100.7.53 (URSHISTSVR01) on port 1433/tcp
10.100.7.53 (URSHISTSVR01) on port 3389/tcp
10.100.6.90 (IT01-FT0Y4Y2) on port 3389/tcp
10.100.6.81 (IT01-CX9WNW1) on port 3389/tcp
10.100.6.65 (IT01-B11Y4Y2) on port 3389/tcp
10.100.5.64 (CONMSAUTHMI601) on port 1433/tcp
10.100.5.64 (CONMSAUTHMI601) on port 3389/tcp
10.100.6.20 on port 443/tcp
10.100.5.68 (IT02-2SD5Y2) on port 1433/tcp
10.100.5.68 (IT02-2SD5Y2) on port 3389/tcp
10.100.5.60 (IT08-DF9HLW2) on port 3389/tcp
10.100.5.58 on port 443/tcp
10.100.2.60 on port 443/tcp
10.100.2.57 on port 443/tcp

	10.100.2.56 on port 443/tcp 10.100.2.53 (it05-100625) on port 8191/tcp 10.100.2.45 on port 443/tcp 10.100.1.151 on port 443/tcp 10.100.1.150 on port 443/tcp 10.100.3.64 (IT01-4P775Y2) on port 3389/tcp 10.100.3.57 on port 443/tcp 10.100.3.52 (IT10-CM1V8Y1) on port 3389/tcp 10.100.3.51 (IT03-4M7MM32) on port 3389/tcp 10.100.2.93 (IT10-DHVDT13) on port 3389/tcp 10.100.2.81 (WindUtilWS) on port 3389/tcp 10.100.2.70 (IT09-6GRJN53) on port 443/tcp 10.100.2.60 on port 9080/tcp 10.100.2.58 on port 9080/tcp 10.100.2.58 on port 443/tcp 10.100.2.57 on port 9080/tcp 10.100.2.56 on port 9080/tcp 10.100.2.54 (IT09-1KBKLR2) on port 3389/tcp 10.100.2.53 (it05-100625) on port 3389/tcp 10.100.2.53 (it05-100625) on port 8089/tcp 10.100.2.51 on port 8834/tcp 10.100.2.49 (IT09-H42HYV1) on port 3389/tcp 10.100.2.49 (IT09-H42HYV1) on port 443/tcp 10.100.2.45 on port 8443/tcp 10.100.1.99 (IT10-BVMFJX2) on port 3389/tcp 10.100.1.80 on port 8009/tcp 10.100.1.80 on port 8443/tcp 10.100.1.76 (IT10-F8BP2R1) on port 3389/tcp 10.100.1.74 on port 443/tcp
Additional Output	Here is the list of SSL CBC ciphers supported by the remote server : Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES) Name Code KEX Auth Encryption MAC DES-CBC3-SHA 0x00, 0x0A RSA RSA 3DES-CBC(168) SHA1 High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1 ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1 AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1 AES256 ------------ snipped ------------

SSL Compression Methods Supported	
Severity	
Description	This script detects which compression methods are supported by the remote service for SSL connections. The remote service supports one or more compression methods for SSL connections.
Recommendation	n/a
References	http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml https://tools.ietf.org/html/rfc3749 https://tools.ietf.org/html/rfc3943 https://tools.ietf.org/html/rfc5246
Affected Nodes	192.168.2.5 on port 902/tcp 192.168.2.5 on port 5989/tcp 192.168.2.5 on port 443/tcp 192.168.2.3 on port 902/tcp 192.168.2.3 on port 5989/tcp 192.168.2.3 on port 443/tcp 10.100.2.53 (it05-100625) on port 8089/tcp

Additional Output	vPenTest Partner was able to confirm that the following compression method is supported by the target : DEFLATE (0x01)

STUN Detection	
Severity	
Description	The remote service supports the STUN (Session Traversal Utilities for NAT) protocol as described in RFC 5389. STUN helps client software behind a NAT router discover the external public address and the behavior of the router. Note that an earlier version of the protocol used a different acronym - 'Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)' - as specified in RFC 3489. A STUN server is listening on the remote host.
Recommendation	n/a
References	https://en.wikipedia.org/wiki/Session_Traversal_Utilities_for_NAT https://tools.ietf.org/html/rfc5389
Affected Nodes	10.100.35.50 on port 3478/udp 10.100.2.45 on port 3478/udp
Additional Output	MAPPED-ADDRESS = 10.100.2.51:2660 SOURCE-ADDRESS = 0.0.0.0:0 CHANGED-ADDRESS = 0.0.0.0:0

Target Credential Status by Authentication Protocol - No Credentials Provided	
Severity	
Description	vPenTest Partner was not able to successfully authenticate directly to the remote target on an available authentication protocol. vPenTest Partner was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but vPenTest Partner failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details. Please note the following : - This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service. - Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets. vPenTest Partner was able to find common ports used for local checks, however, no credentials were provided in the scan policy.
Recommendation	n/a
References	n/a
Affected Nodes	192.168.2.74 on port 0/tcp 192.168.2.25 on port 0/tcp 192.168.2.22 on port 0/tcp 192.168.2.19 on port 0/tcp 192.168.2.18 on port 0/tcp 192.168.2.8 on port 0/tcp 192.168.2.6 on port 0/tcp 192.168.2.5 on port 0/tcp

10.100.35.104 on port 0/tcp
10.100.35.89 on port 0/tcp
10.100.35.77 on port 0/tcp
10.100.35.72 on port 0/tcp
192.168.2.3 on port 0/tcp
10.100.35.119 on port 0/tcp
10.100.35.51 on port 0/tcp
10.100.34.86 on port 0/tcp
10.100.34.85 on port 0/tcp
10.100.34.83 on port 0/tcp
10.100.34.81 on port 0/tcp
10.100.34.80 on port 0/tcp
10.100.34.77 on port 0/tcp
10.100.34.75 on port 0/tcp
10.100.34.73 on port 0/tcp
10.100.34.72 on port 0/tcp
10.100.34.71 on port 0/tcp
10.100.34.70 on port 0/tcp
10.100.34.69 on port 0/tcp
10.100.34.68 on port 0/tcp
10.100.34.66 on port 0/tcp
10.100.34.65 on port 0/tcp
10.100.34.63 on port 0/tcp
10.100.34.62 on port 0/tcp
10.100.34.60 on port 0/tcp
10.100.34.59 on port 0/tcp
10.100.34.58 on port 0/tcp
10.100.34.57 on port 0/tcp
10.100.34.55 on port 0/tcp
10.100.34.54 on port 0/tcp
10.100.34.53 on port 0/tcp
10.100.34.52 on port 0/tcp
10.100.34.51 on port 0/tcp
10.100.34.50 on port 0/tcp
10.100.33.59 on port 0/tcp
10.100.34.79 on port 0/tcp
10.100.34.78 on port 0/tcp
10.100.34.76 on port 0/tcp
10.100.34.74 on port 0/tcp
10.100.34.67 on port 0/tcp
10.100.34.64 on port 0/tcp
10.100.34.61 on port 0/tcp
10.100.34.56 on port 0/tcp
10.100.33.55 on port 0/tcp
10.100.33.54 on port 0/tcp
10.100.33.53 on port 0/tcp
10.100.33.50 on port 0/tcp
10.100.32.69 on port 0/tcp
10.100.32.65 on port 0/tcp
10.100.32.63 on port 0/tcp
10.100.32.62 on port 0/tcp
10.100.32.61 on port 0/tcp
10.100.32.59 on port 0/tcp
10.100.32.58 on port 0/tcp
10.100.32.57 on port 0/tcp
10.100.32.56 on port 0/tcp
10.100.32.55 on port 0/tcp
10.100.32.54 on port 0/tcp
10.100.32.53 on port 0/tcp
10.100.32.52 on port 0/tcp
10.100.32.51 on port 0/tcp
10.100.32.50 on port 0/tcp
10.100.31.80 on port 0/tcp
10.100.31.77 on port 0/tcp
10.100.31.75 on port 0/tcp
10.100.31.73 on port 0/tcp
10.100.31.71 on port 0/tcp
10.100.31.70 on port 0/tcp
10.100.31.67 on port 0/tcp

10.100.31.61 on port 0/tcp
10.100.31.59 on port 0/tcp
10.100.31.58 on port 0/tcp
10.100.31.56 on port 0/tcp
10.100.31.55 on port 0/tcp
10.100.31.53 on port 0/tcp
10.100.31.51 on port 0/tcp
10.100.31.50 on port 0/tcp
10.100.20.200 on port 0/tcp
10.100.20.195 on port 0/tcp
10.100.20.145 on port 0/tcp
10.100.20.38 (ssd505) on port 0/tcp
10.100.20.33 (lt186) on port 0/tcp
10.100.20.11 on port 0/tcp
10.100.20.7 on port 0/tcp
10.100.7.210 on port 0/tcp
10.100.7.201 on port 0/tcp
10.100.7.135 on port 0/tcp
10.100.7.131 on port 0/tcp
10.100.7.125 on port 0/tcp
10.100.7.119 on port 0/tcp
10.100.7.118 on port 0/tcp
10.100.7.116 on port 0/tcp
10.100.7.115 on port 0/tcp
10.100.7.111 on port 0/tcp
10.100.7.110 on port 0/tcp
10.100.7.101 (SmartTool-TMP) on port 0/tcp
10.100.7.98 on port 0/tcp
10.100.7.97 on port 0/tcp
10.100.7.96 on port 0/tcp
10.100.20.2 on port 0/tcp
10.100.7.136 on port 0/tcp
10.100.7.90 (HMI-01B) on port 0/tcp
10.100.7.88 (URSIOSSVR01) on port 0/tcp
10.100.7.87 (SmartTool) on port 0/tcp
10.100.7.86 (HIST-01A) on port 0/tcp
10.100.7.85 (MPM) on port 0/tcp
10.100.7.84 (HMI1) on port 0/tcp
10.100.7.82 (TESTPC06) on port 0/tcp
10.100.7.78 (OSSEM3_RIUHMI01) on port 0/tcp
10.100.7.77 (HMI-01A) on port 0/tcp
10.100.7.75 (IT03-5D3BVV1) on port 0/tcp
10.100.7.74 on port 0/tcp
10.100.7.73 (VSS-01A) on port 0/tcp
10.100.7.72 (DESKTOP-KOCHTQC) on port 0/tcp
10.100.7.71 (VSS-01B) on port 0/tcp
10.100.7.70 (EWS-01) on port 0/tcp
10.100.7.69 on port 0/tcp
10.100.7.66 (URSIOSSVR02) on port 0/tcp
10.100.7.62 (OSSEM2_RIOHMI01) on port 0/tcp
10.100.7.53 (URSHISTSVR01) on port 0/tcp
10.100.7.51 (it03-8ddvdv1) on port 0/tcp
10.100.7.50 (IT02-8ZWM353) on port 0/tcp
10.100.6.92 (IT01-1K7FLR2) on port 0/tcp
10.100.6.90 (IT01-FT0Y4Y2) on port 0/tcp
10.100.6.84 (IT01-G9S2YM2) on port 0/tcp
10.100.6.81 (IT01-CX9WNW1) on port 0/tcp
10.100.6.80 (IT01-486J8V1-Wiring-PC) on port 0/tcp
10.100.6.69 (IT01-9WQ7HD1) on port 0/tcp
10.100.6.68 (IT01-CMCW8Y1) on port 0/tcp
10.100.6.66 (IT01-GS97L02) on port 0/tcp
10.100.6.65 (IT01-B11Y4Y2) on port 0/tcp
10.100.7.95 (IT09-5Z5KN53) on port 0/tcp
10.100.6.62 (IT01-486G8V1) on port 0/tcp
10.100.6.60 (IT01-2VDFG12) on port 0/tcp
10.100.6.53 (IT01-8NQH353) on port 0/tcp
10.100.6.50 (IT02-FGXJ842) on port 0/tcp
10.100.5.68 (IT02-2SD5Y2) on port 0/tcp
10.100.5.67 (IT02-4RWKQ13) on port 0/tcp

	10.100.5.64 (CONMSAUTHMI601) on port 0/tcp 10.100.5.62 (IT02-DWCKN53) on port 0/tcp 10.100.5.61 (IT02-34HR733) on port 0/tcp 10.100.5.60 (IT08-DF9HLW2) on port 0/tcp 10.100.5.59 (IT06-G8F8HF1) on port 0/tcp 10.100.5.58 on port 0/tcp 10.100.5.56 (IT02-GS5WZY2) on port 0/tcp 10.100.5.55 (IT09-5Z5KN53) on port 0/tcp 10.100.5.53 on port 0/tcp 10.100.5.52 on port 0/tcp 10.100.5.51 (IT03-75NWST2) on port 0/tcp 10.100.6.57 (IT01-8WWKQ13) on port 0/tcp 10.100.3.64 (IT01-4P775Y2) on port 0/tcp 10.100.3.56 (IT02-FNFR2R1) on port 0/tcp 10.100.3.53 on port 0/tcp 10.100.3.51 (IT03-4M7MM32) on port 0/tcp 10.100.2.93 (IT10-DHVDT13) on port 0/tcp 10.100.2.83 (Training2) on port 0/tcp 10.100.2.82 (Training8) on port 0/tcp 10.100.2.70 (IT09-6GRJN53) on port 0/tcp 10.100.2.66 (IT10-34S1MQ1) on port 0/tcp 10.100.2.65 (IT09-JGYQ733) on port 0/tcp 10.100.2.64 (it10-g0wtsw1) on port 0/tcp 10.100.2.63 (WIN-NLN1IU84VKS) on port 0/tcp 10.100.2.62 on port 0/tcp 10.100.2.60 on port 0/tcp 10.100.2.59 (WIN-NLN1IU84VKS) on port 0/tcp 10.100.2.58 on port 0/tcp 10.100.2.57 on port 0/tcp 10.100.2.56 on port 0/tcp 10.100.2.55 (Training3) on port 0/tcp 10.100.2.53 (it05-100625) on port 0/tcp 10.100.2.52 (WIN-NLN1IU84VKS) on port 0/tcp 10.100.2.51 on port 0/tcp 10.100.2.49 (IT09-H42HYV1) on port 0/tcp 10.100.2.45 on port 0/tcp 10.100.1.99 (IT10-BVMFJX2) on port 0/tcp 10.100.1.97 (IT10-37HWTR1) on port 0/tcp 10.100.1.96 on port 0/tcp 10.100.1.76 (IT10-F8BP2R1) on port 0/tcp 10.100.1.68 (IT10-F20GXV1) on port 0/tcp 10.100.1.66 (IT10--HNGWST2) on port 0/tcp
Additional Output	`SMB was detected on port 445 but no credentials were provided.` `SMB local checks were not enabled.`

TeamViewer remote detection	
Severity	
Description	TeamViewer, a remote control service, is installed on the remote Windows host. A TeamViewer service has been detected on the remote host.
Recommendation	n/a
References	https://www.teamviewer.com/en/
Affected Nodes	10.100.7.70 (EWS-01) on port 0/tcp

Additional Output	`Path    : /`
	`  Version : unknown`
	`  Product : TeamViewer`

Telnet Server Detection	
Severity	

Description	The remote host is running a Telnet server, a remote terminal server. A Telnet server is listening on the remote port.
Recommendation	Disable this service if you do not use it.
References	n/a
Affected Nodes	192.168.2.2 on port 60000/tcp 10.100.35.5 on port 23/tcp 10.100.34.15 on port 23/tcp 10.100.34.5 on port 23/tcp 10.100.33.15 on port 23/tcp 10.100.33.5 on port 23/tcp 10.100.32.15 on port 23/tcp 10.100.32.5 on port 23/tcp 10.100.31.5 on port 23/tcp 10.100.7.74 on port 23/tcp 10.100.7.64 on port 23/tcp 10.100.7.63 on port 23/tcp 10.100.7.5 on port 23/tcp 10.100.6.26 on port 9999/tcp 10.100.6.5 on port 23/tcp 10.100.5.58 on port 23/tcp 10.100.5.25 on port 23/tcp 10.100.5.5 on port 23/tcp 10.100.4.5 on port 23/tcp 10.100.3.25 on port 23/tcp 10.100.3.5 on port 23/tcp 10.100.2.5 on port 23/tcp 10.100.1.25 on port 23/tcp 10.100.1.5 on port 23/tcp

Additional Output	`Here is the banner from the remote Telnet server :`
	
	`------------------------------ snip ------------------------------`
	
	`>`
	`------------------------------ snip ------------------------------`

TLS Version 1.3 Protocol Detection	
Severity	
Description	The remote service accepts connections encrypted using TLS 1.3. The remote service encrypts traffic using a version of TLS.
Recommendation	N/A
References	https://tools.ietf.org/html/rfc8446
Affected Nodes	10.100.35.50 on port 443/tcp 10.100.31.82 on port 443/tcp 10.100.31.81 on port 443/tcp 10.100.31.69 on port 443/tcp 10.100.31.69 on port 5061/tcp 10.100.31.60 on port 443/tcp 10.100.31.52 on port 443/tcp 10.100.31.54 on port 443/tcp 10.100.7.69 on port 443/tcp 10.100.2.51 on port 8834/tcp
Additional Output	`TLSv1.3 is enabled and the server supports at least one cipher.`

Universal Plug and Play (UPnP) Protocol Detection	
Severity	

	
Description	The remote device answered an SSDP M-SEARCH request. Therefore, it supports 'Universal Plug and Play' (UPnP). This protocol provides automatic configuration and device discovery. It is primarily intended for home networks. An attacker could potentially leverage this to discover your network architecture. The remote device supports UPnP.
Recommendation	Filter access to this port if desired.
References	https://en.wikipedia.org/wiki/Universal_Plug_and_Play https://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol http://quimby.gnus.org/internet-drafts/draft-cai-ssdp-v1-03.txt
Affected Nodes	192.168.2.17 on port 1900/udp 10.100.35.73 on port 1900/udp 10.100.35.50 on port 1900/udp 10.100.33.20 on port 1900/udp 10.100.31.82 on port 1900/udp 10.100.31.81 on port 1900/udp 10.100.31.69 on port 1900/udp 10.100.31.60 on port 1900/udp 10.100.31.54 on port 1900/udp 10.100.31.52 on port 1900/udp 10.100.7.150 on port 1900/udp 10.100.6.87 on port 1900/udp 10.100.6.20 on port 1900/udp 10.100.3.150 on port 1900/udp 10.100.3.151 on port 1900/udp 10.100.2.45 on port 1900/udp 10.100.1.151 on port 1900/udp 10.100.1.150 on port 1900/udp 10.100.1.80 on port 1900/udp

Additional Output	`The device responded to an SSDP M-SEARCH request with the following locations :`
	
	`http://192.168.2.17:80/upnp.jsp`
	
	`And advertises these unique service names :`
	
	`uuid:6f2e64a2-8ffa-40eb-abfc-C08ADE1D5F70::upnp:rootdevice`

VMWare STARTTLS Support	
Severity	
Description	The remote VMWare server supports the use of encryption initiated during pre-login to switch from a cleartext to an encrypted communications channel. The remote service supports encrypting traffic.
Recommendation	n/a
References	n/a
Affected Nodes	192.168.2.5 on port 902/tcp 192.168.2.3 on port 902/tcp 10.100.5.51 (IT03-75NWST2) on port 902/tcp

Additional Output	`Here is the VMWare's SSL certificate that vPenTest Partner`
	`was able to collect after sending a pre-login packet :`
	
	`------------------------------ snip ------------------------------`
	`Subject Name:`
	
	`Country: US`
	`State/Province: California`
	`Locality: Palo Alto`
	`Organization: VMware, Inc`
	`Organization Unit: VMware ESX Server Default Certificate`
	`Email Address: ssl-certificates@vmware.com`

```
Common Name: localhost.localdomain
Unstructured Name: 1424180350,564d7761726520496e632e

Issuer Name:

Organization: VMware Installer

Serial Number: 5A 17 31 34 17 B4

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Feb 17 13:39:11 2015 GMT
Not Valid After: Aug 18 13:39:11 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C6 9D A6 EF FC 4B C0 2A 96 E1 0D 6E 04 8E 97 8F C3 29 94
            5E 62 1F AC 06 D4 47 6F F6 29 37 D5 76 28 17 A6 24 9C 8F 29
            C0 05 39 03 B6 1C 6F 76 36 8F 97 59 B4 D1 73 6B 56 FC 20 88
            84 DA F6 75
------------ snipped ------------
```

VNC Server Unencrypted Communication Detection	
Severity	
Description	This script checks the remote VNC server protocol version and the available 'security types' to determine if any unencrypted 'security-types' are in use or available. A VNC server with one or more unencrypted 'security-types' is running on the remote host.
Recommendation	n/a
References	n/a
Affected Nodes	192.168.2.73 on port 5900/tcp 192.168.2.70 on port 5900/tcp 192.168.2.97 on port 5900/tcp 192.168.2.81 on port 5900/tcp 192.168.2.77 on port 5900/tcp 10.100.35.89 on port 5900/tcp 10.100.34.85 on port 5900/tcp 10.100.33.61 on port 5900/tcp 10.100.33.59 on port 5900/tcp 10.100.33.54 on port 5900/tcp 10.100.32.65 on port 5900/tcp 10.100.20.33 (lt186) on port 5900/tcp 10.100.7.201 on port 5900/tcp 10.100.6.90 (IT01-FT0Y4Y2) on port 5900/tcp 10.100.6.65 (IT01-B11Y4Y2) on port 5900/tcp 10.100.5.68 (IT02-2SD5Y2) on port 5900/tcp 10.100.5.60 (IT08-DF9HLW2) on port 5900/tcp 10.100.3.64 (IT01-4P775Y2) on port 5900/tcp 10.100.3.52 (IT10-CM1V8Y1) on port 5900/tcp 10.100.2.93 (IT10-DHVDT13) on port 5900/tcp 10.100.2.81 (WindUtilWS) on port 5900/tcp 10.100.2.66 (IT10-34S1MQ1) on port 5900/tcp 10.100.2.54 (IT09-1KBKLR2) on port 5900/tcp 10.100.2.53 (it05-100625) on port 5900/tcp 10.100.1.99 (IT10-BVMFJX2) on port 5900/tcp 10.100.1.76 (IT10-F8BP2R1) on port 5900/tcp
Additional Output	`The remote VNC server supports the following security types which do not perform full data communication encryption by default and thus should be checked to ensure that full data encryption is enabled :`

	30 (Mac OSX SecType 30) 35 (Mac OSX SecType 35)

WebDAV Detection	
Severity	
Description	WebDAV is an industry standard extension to the HTTP specification. It adds a capability for authorized users to remotely add and manage the content of a web server. If you do not use this extension, you should disable it.
Recommendation	http://support.microsoft.com/default.aspx?kbid=241520
References	n/a
Affected Nodes	192.168.2.6 on port 80/tcp 10.100.7.110 on port 80/tcp
Additional Output	n/a

Web Server UPnP Detection	
Severity	
Description	vPenTest Partner was able to extract some information about the UPnP-enabled device by querying this web server. Services may also be reachable through SOAP requests. The remote web server provides UPnP information.
Recommendation	Filter incoming traffic to this port if desired.
References	https://en.wikipedia.org/wiki/Universal_Plug_and_Play
Affected Nodes	10.100.35.73 on port 1393/tcp 10.100.35.73 on port 1223/tcp 192.168.2.17 on port 80/tcp 10.100.35.73 on port 1093/tcp 10.100.35.73 on port 1468/tcp 10.100.33.20 on port 49152/tcp 10.100.31.82 on port 49152/tcp 10.100.31.81 on port 49152/tcp 10.100.31.69 on port 49152/tcp 10.100.31.60 on port 49152/tcp 10.100.31.54 on port 49152/tcp 10.100.31.52 on port 49152/tcp 10.100.7.150 on port 49152/tcp 10.100.6.87 on port 49152/tcp 10.100.6.20 on port 49152/tcp 10.100.3.151 on port 49152/tcp 10.100.3.150 on port 49152/tcp 10.100.1.151 on port 49152/tcp 10.100.1.150 on port 49152/tcp 10.100.1.80 on port 8008/tcp
Additional Output	Here is a summary of http://192.168.2.17:80/upnp.jsp : deviceType: urn:schemas-upnp-org:device:InternetGatewayDevice:1 friendlyName: ZoneDirector 192.168.2.17 manufacturer: Ruckus Wireless manufacturerURL: http://www.ruckuswireless.com modelName: ZD1106 modelDescription: Ruckus Wireless ZoneDirector modelName: ZD1106 modelNumber: 9.4.3.0 modelURL: http://www.ruckuswireless.com/ serialNumber: 161323000755 ServiceID: urn:upnp-org:serviceId:Basic1

```
        serviceType: urn:schemas-upnp-org:service:WirelessSwitch:1
        controlURL: /upnp/control/Basic1
        eventSubURL: /upnp/event/Basic1
        SCPDURL: /BasicSCPD.xml
```