Qualys. Enterprise

PCI report

February 04, 2019

This report was generated with an evaluation version of

Executive Summary

This report is not eligible for PCI certification. Please use QualysGuard PCI (via your linked account) to generate certified PCI reports.

PCI Status

According to PCI DSS v3.0 Requirement 6.1, merchants are required to fix all High ranking vulnerabilities according to a risk ranking scale. This scale can be customized using the report template.

Total count of High vulnerabilities	2

Live IP Addresses Scanned	Security Risk Rating	Number of vulnerabilities with High severity
10.10.32.86	3.0	2

Report Summary	
User Name:	Pavel Sotnikov
Login Name:	tamde_ps
Company:	TAM Demo Account
User Role:	Manager
Address:	1600 Bridge Parkway
City:	Redwood Shores
State:	California
Zip:	94065
Country:	United States of America
Created:	02/04/2019 at 01:59:49 AM (GMT-0500)
Template Title:	Macy's PCI Template
Asset Groups:	10.10.32.86
IPs:	-
Sort by:	Host
Trend Analysis:	Latest vulnerability data
Date Range:	12/31/1998 - 02/04/2019
Active Hosts:	1
Hosts Matching Filters:	1

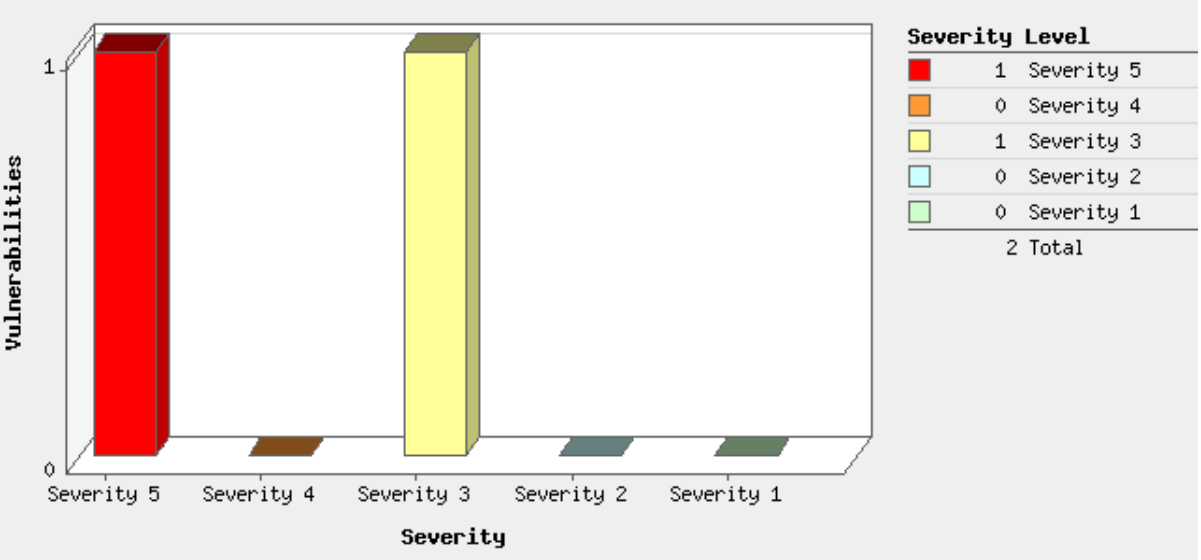
Summary of Vulnerabilities

Vulnerabilities Total	29	Security Risk (Avg)	3.0	Business Risk	16/100

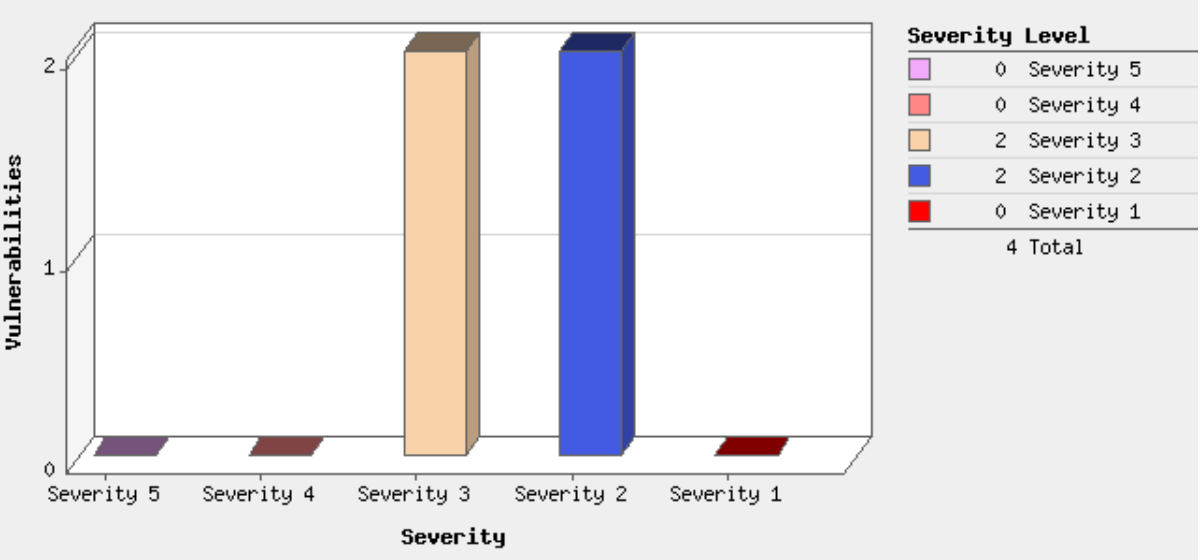
by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	1	0	0	1
4	0	0	0	0
3	1	2	1	4
2	0	2	4	6
1	0	0	18	18
Total	2	4	23	29

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
General remote services	0	4	6	10
TCP/IP	0	0	5	5
Information gathering	0	0	5	5
Windows	1	0	2	3
Security Policy	1	0	1	2
Total	2	4	19	25

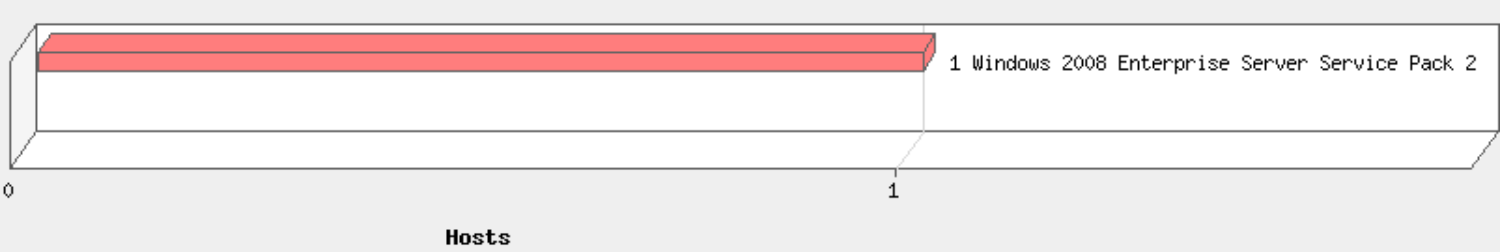
Vulnerabilities by Severity



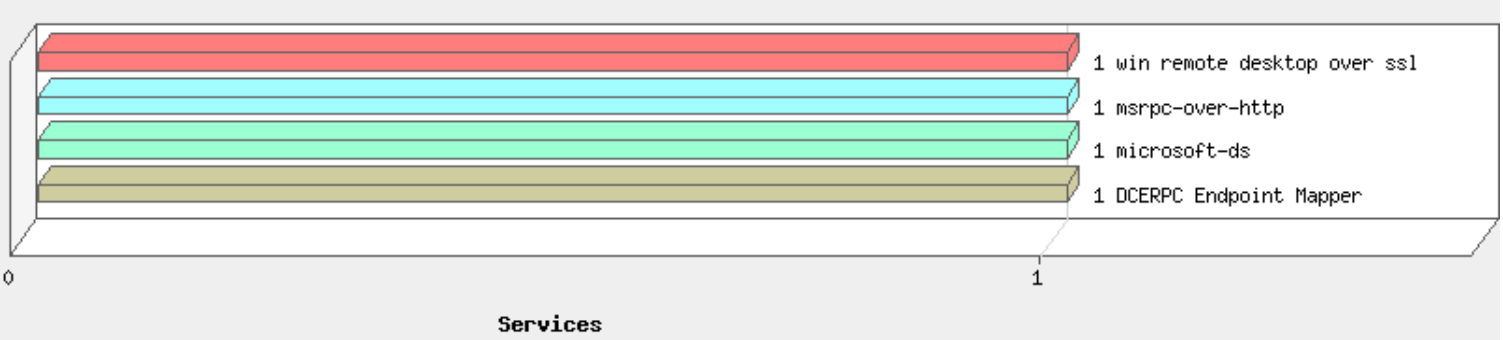
Potential Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

10.10.32.86 (com-2k8-32-86, COM-2K8-32-86) Windows 2008 Enterprise Server Service Pack 2
Global Default Network cpe:/o:microsoft:windows_server_2008::sp2:enterprise_x64:

Vulnerabilities Total	29	Security Risk	3.0

by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	1	0	0	1
4	0	0	0	0
3	1	2	1	4
2	0	2	4	6
1	0	0	18	18
Total	2	4	23	29

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
General remote services	0	4	6	10
TCP/IP	0	0	5	5
Information gathering	0	0	5	5
Windows	1	0	2	3
Security Policy	1	0	1	2
Total	2	4	19	25

Vulnerabilities (2)

Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020) CVSS: 2 CVSS3: - Active

PCI COMPLIANCE STATUS

PCI Severity: HIGH

VULNERABILITY DETAILS

CVSS Base Score:	**9.3**	AV:N/AC:M/Au:N/C:C/I:C/A:C
CVSS Temporal Score:	**7.7**	E:F/RL:OF/RC:C
CVSS3 Base Score:	-	
CVSS3 Temporal Score:	-	
Severity:	**5**	
QID:	90783	
Category:	Windows	
CVE ID:	CVE-2012-0002, CVE-2012-0152	
Vendor Reference:	MS12-020	
Bugtraq ID:	52354	
Service Modified:	03/29/2012	
User Modified:	-	
Edited:	No	
PCI Vuln:	Yes	
Ticket State:	Open	

First Detected: 03/17/2012 at 03:00:19 AM (GMT-0400)

Last Detected: 09/19/2016 at 10:08:35 AM (GMT-0400)

Times Detected: 423

Last Fixed: 05/23/2013 at 01:03:15 AM (GMT-0400)

CVSS Environment:

Asset Group:	10.10.32.86
Collateral Damage Potential:	Low
Target Distribution:	Low
Confidentiality Requirement:	High
Integrity Requirement:	High
Availability Requirement:	High

THREAT:

The Remote Desktop feature in Windows enables access to all of the programs, resources and accessories on a user's computer from a second Windows-based computer.
A remote code execution vulnerability exists in the way the Remote Desktop Protocol accesses an object in memory that has been improperly initialized or has been deleted (CVE-2012-0002).
A denial of service vulnerability exists in the way the Remote Desktop Protocol service processes packets. An attacker who successfully exploited this vulnerability could cause the target service to stop responding (CVE-2012-0152).
This security update is rated Critical for all supported releases of Microsoft Windows.
Note:
NLA or network layer authentication is a layer of security on top of RDP. If NLA is enabled then the vulnerability can be exploited remotely but will need credentials.
1. The authenticated check will determine presence of this vulnerability irrespective of the NLA setting.
2. The remote check can determine presence of this vulnerability only if NLA is disabled.
We encourage customers to patch irrespective of the NLA status.
Windows Embedded Systems:- For additional information regarding security updates for embedded systems, refer to the following MSDN blog(s):
March 2012 Security Updates for XPe SP3 and Standard 2009 Are Now on ECE (http://blogs.msdn.com/b/embedded/archive/2012/03/26/march-2012-security-updates-for-xpe-sp3-and-standard-2009-are-now-on-ece.aspx) (KB2621440)
April 2012 Security Updates are Live on ECE for XPe and Standard 2009 (http://blogs.msdn.com/b/embedded/archive/2012/04/24/april-2012-security-updates-are-live-on-ece-for-xpe-and-standard-2009.aspx) (KB2621440)

Note: This vulnerability is applicable to versions of the software that are not listed in the official advisory.

IMPACT:

Successfully exploiting these vulnerabilities might allow a remote attacker to execute arbitrary code or cause a denial of service.

SOLUTION:

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MS12-020: Windows XP Service Pack 3 (http://www.microsoft.com/downloads/details.aspx?familyid=18a1fe48-1318-4b93-afad-206950bb1ae5)
MS12-020: Windows XP Professional x64 Edition Service Pack 2 (http://www.microsoft.com/downloads/details.aspx?familyid=eccf865d-399a-4862-b26f-f35580419875)
MS12-020: Windows Server 2003 Service Pack 2 (http://www.microsoft.com/downloads/details.aspx?familyid=b69b4b9b-c0a1-4c1e-b081-8529eaf1536a)
MS12-020: Windows Server 2003 x64 Edition Service Pack 2 (http://www.microsoft.com/downloads/details.aspx?familyid=8081e67f-288c-4714-bff8-e0ff9777692f)
MS12-020: Windows Server 2003 with SP2 for Itanium-based Systems (http://www.microsoft.com/downloads/details.aspx?familyid=521baa02-5d7a-4cba-8a1a-2af1b6e4cbe4)
MS12-020: Windows Vista Service Pack 2 (http://www.microsoft.com/downloads/details.aspx?familyid=39abdf7b-ea9d-4b95-a28d-4140374d531d)
MS12-020: Windows Vista x64 Edition Service Pack 2 (http://www.microsoft.com/downloads/details.aspx?familyid=e5970daf-4440-42fa-8efc-e6190c6a22aa)
MS12-020: Windows Server 2008 for 32-bit Systems Service Pack 2 (http://www.microsoft.com/downloads/details.aspx?familyid=fef2c1d7-2004-43d7-aa49-673c6f374670)
MS12-020: Windows Server 2008 for x64-based Systems Service Pack 2 (http://www.microsoft.com/downloads/details.aspx?familyid=4ffae13f-3432-4849-a2da-a76f96d7ceb3)
MS12-020: Windows Server 2008 for Itanium-based Systems Service Pack 2 (http://www.microsoft.com/downloads/details.aspx?familyid=67581250-50fd-4f4c-a3cc-45ce2662b0c3)
MS12-020: Windows 7 for 32-bit Systems and Windows 7 for 32-bit Systems Service Pack 1 (http://www.microsoft.com/downloads/details.aspx?familyid=16b0195c-84d3-4c08-8b98-ff2c80d144e1)
MS12-020: Windows 7 for 32-bit Systems and Windows 7 for 32-bit Systems Service Pack 1 (http://www.microsoft.com/downloads/details.aspx?familyid=3a6c7fdf-105a-4886-ad52-c892f37e32d1)
MS12-020: Windows 7 for x64-based Systems and Windows 7 for x64-based Systems Service Pack 1 (http://www.microsoft.com/downloads/details.aspx?familyid=40b62d08-d2a2-4900-b01c-46fc761973d0)
MS12-020: Windows 7 for x64-based Systems and Windows 7 for x64-based Systems Service Pack 1 (http://www.microsoft.com/downloads/details.aspx?familyid=1bbe7cda-4bee-4d65-8127-3c13624a1168)
MS12-020: Windows Server 2008 R2 for x64-based Systems and Windows Server 2008 R2 for x64-based Systems Service Pack 1* (http://www.microsoft.com/downloads/details.aspx?familyid=7c1774cc-e00c-47f3-97a2-bc90de857793)
MS12-020: Windows Server 2008 R2 for x64-based Systems and Windows Server 2008 R2 for x64-based Systems Service Pack 1* (http://www.microsoft.com/downloads/details.aspx?familyid=7ec21f41-1673-4592-b45c-6438ad57e08c)
MS12-020: Windows Server 2008 R2 for Itanium-based Systems and Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (http://www.microsoft.com/downloads/details.aspx?familyid=6a07f99c-8ab4-4e44-8d48-6ac787dd2b51)
MS12-020: Windows Server 2008 R2 for Itanium-based Systems and Windows Server 2008 R2 for Itanium-based Systems Service Pack 1 (http://www.microsoft.com/downloads/details.aspx?familyid=469aa1f6-ed89-4649-8736-eaa5e2ad44ee)

RESULTS:

QID: 90783 detected on port 3389 over TCP.

Microsoft Remote Desktop Service Not Using Additional Encryption

CVSS: 1.5 CVSS3: - Active

PCI COMPLIANCE STATUS

PCI Severity: MED

VULNERABILITY DETAILS

CVSS Base Score:	**5.8** [1] AV:N/AC:M/Au:N/C:P/I:P/A:N
CVSS Temporal Score:	**4.7** E:U/RL:W/RC:C
CVSS3 Base Score:	-
CVSS3 Temporal Score:	-
Severity:	**3**
QID:	105500
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/25/2013
User Modified:	-
Edited:	No
PCI Vuln:	Yes
Ticket State:	Open

First Detected: 04/27/2013 at 03:01:24 AM (GMT-0400)

Last Detected: 09/19/2016 at 10:08:35 AM (GMT-0400)

Times Detected: 160

Last Fixed: N/A

CVSS Environment:

Asset Group:	10.10.32.86
Collateral Damage Potential:	Low
Target Distribution:	Low
Confidentiality Requirement:	High
Integrity Requirement:	High
Availability Requirement:	High

THREAT:

The Remote Desktop feature in Windows enables access to all of the programs, resources and accessories on a user's computer from a second Windows-based computer.
By default, Remote Desktop Services sessions are configured to negotiate the encryption level from the client to the RD Session Host server. The security of Remote Desktop Services sessions can be enhanced by requiring the use of Transport Layer Security (TLS) 1.0.
TLS 1.0 verifies the identity of the Remote Desktop Session Host server and encrypts all communication between the Remote Desktop Session Host server and the client computer. The Remote Desktop Session Host server and the client computer must be correctly configured for TLS to provide enhanced security.

IMPACT:

Successfully exploiting this vulnerability might allow a remote attacker to cause man-in-the-middle attacks

SOLUTION:

Workaround:
Configure Remote Desktop to work over SSL/TLS. Refer Microsoft Technet Article cc770833 (http://technet.microsoft.com/en-us/library/cc770833.aspx) and Microsoft Technet Article cc782610 (http://technet.microsoft.com/en-us/library/cc782610.aspx)

RESULTS:

QID: 105500 detected on port 3389 over TCP.

Potential Vulnerabilities (4)

SSL/TLS Server supports TLSv1.0 — port 3389/tcp over SSL — CVSS: 1.3 — CVSS3: - — New

PCI COMPLIANCE STATUS

PCI Severity: MED

VULNERABILITY DETAILS

CVSS Base Score:	**4.3** [1] AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.9** E:F/RL:W/RC:C
CVSS3 Base Score:	-
CVSS3 Temporal Score:	-
Severity:	**3**
QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	12/20/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes
Ticket State:	Open

First Detected: 09/19/2016 at 10:08:35 AM (GMT-0400)
Last Detected: 09/19/2016 at 10:08:35 AM (GMT-0400)
Times Detected: 1
Last Fixed: N/A

CVSS Environment:

Asset Group:	10.10.32.86
Collateral Damage Potential:	Low
Target Distribution:	Low
Confidentiality Requirement:	High
Integrity Requirement:	High
Availability Requirement:	High

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.
This QID is an automatic PCI FAIL in accordance with the PCI standards.
Further details can be found under:
PCI: ASV Program Guide v3.1 (page 27) (https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf)
PCI: Use of SSL Early TLS and ASV Scans (https://www.pcisecuritystandards.org/documents/Use-of-SSL-Early-TLS-and-ASV-Scans.pdf)

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:
openssl s_client -connect ip:port -tls1

If the test is successful, then the target support TLSv1

RESULTS:

TLSv1.0 is supported

SSL/TLS use of weak RC4 cipher — port 3389/tcp over SSL — CVSS: 1.3 — CVSS3: 5.4 — Active

PCI COMPLIANCE STATUS

PCI Severity: MED

VULNERABILITY DETAILS

CVSS Base Score:	**4.3**	AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**3.7**	E:POC/RL:W/RC:C
CVSS3 Base Score:	**5.9**	AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS3 Temporal Score:	**5.4**	E:POC/RL:W/RC:C
Severity:	**3**	
QID:	38601	
Category:	General remote services	
CVE ID:	CVE-2013-2566, CVE-2015-2808	
Vendor Reference:	-	
Bugtraq ID:	91787, 58796, 73684	
Service Modified:	10/25/2018	
User Modified:	-	
Edited:	No	
PCI Vuln:	No	

Ticket State: Open

First Detected: 10/19/2013 at 03:01:28 AM (GMT-0400)
Last Detected: 09/19/2016 at 10:08:35 AM (GMT-0400)
Times Detected: 29
Last Fixed: N/A

CVSS Environment:

Asset Group:	10.10.32.86
Collateral Damage Potential:	Low
Target Distribution:	Low
Confidentiality Requirement:	High
Integrity Requirement:	High
Availability Requirement:	High

THREAT:
Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features.
SSL/TLS protocols use ciphers such as AES,DES, 3DES and RC4 to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that the there is a stronger bias in RC4, which make statistical analysis of ciphertext more practical.
The described attack is to inject a malicious javascript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples, that can be used for statistical analysis.
NOTE: On 3/12/15 NVD changed the CVSS v2 access complicity from high to medium. As a result Qualys revised the CVSS score to 4.3 immediately. On 5/4/15 Qualys is also revising the severity to level 3.

IMPACT:
If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.
This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from cihpertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

SOLUTION:
RC4 should not be used where possible. One reason that RC4 was still being used was BEAST and Lucky13 attacks against CBC mode ciphers in SSL and
TLS. However, TLSv 1.2 or later address these issues.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1 WITH RC4 CIPHERs IS SUPPORTED					
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM

SSL Certificate - Signature Verification Failed Vulnerability port 3389/tcp over SSL CVSS: 1.9 CVSS3: - Active

PCI COMPLIANCE STATUS

PCI Severity: HIGH

VULNERABILITY DETAILS

CVSS Base Score: **9.4** [1] AV:N/AC:L/Au:N/C:C/I:C/A:N
CVSS Temporal Score: **6.8** E:U/RL:W/RC:UC
CVSS3 Base Score: -
CVSS3 Temporal Score: -
Severity: **2**
QID: 38173
Category: General remote services

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/25/2018
User Modified:	-
Edited:	No
PCI Vuln:	Yes
Ticket State:	Open

First Detected: 05/11/2013 at 03:01:20 AM (GMT-0400)

Last Detected: 09/19/2016 at 10:08:35 AM (GMT-0400)

Times Detected: 153

Last Fixed: N/A

CVSS Environment:

Asset Group:	10.10.32.86
Collateral Damage Potential:	Low
Target Distribution:	Low
Confidentiality Requirement:	High
Integrity Requirement:	High
Availability Requirement:	High

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.
If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.
Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULTS:

Certificate #0 CN=com-2k8-32-86 unable to get local issuer certificate

SSL Certificate - Subject Common Name Does Not Match Server FQDN port 3389/tcp over SSL CVSS: 0.9 CVSS3: - Active

PCI COMPLIANCE STATUS

PCI Severity: LOW

VULNERABILITY DETAILS

CVSS Base Score:	**2.6** [1] AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	**2.1** E:U/RL:W/RC:C
CVSS3 Base Score:	-
CVSS3 Temporal Score:	-
Severity:	**2**
QID:	38170
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/25/2018
User Modified:	-

Edited:	No
PCI Vuln:	No
Ticket State:	Open

First Detected: 05/11/2013 at 03:01:20 AM (GMT-0400)

Last Detected: 09/19/2016 at 10:08:35 AM (GMT-0400)

Times Detected: 153

Last Fixed: N/A

CVSS Environment:

Asset Group:	10.10.32.86
Collateral Damage Potential:	Low
Target Distribution:	Low
Confidentiality Requirement:	High
Integrity Requirement:	High
Availability Requirement:	High

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.
A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.
Please note that a false positive reporting of this vulnerability is possible in the following case:
If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

RESULTS:

Certificate #0 CN=com-2k8-32-86 (com-2k8-32-86) doesn't resolve

Information Gathered (23)

Remote Access or Management Service Detected

PCI COMPLIANCE STATUS

PCI Severity: LOW

VULNERABILITY DETAILS

CVSS Base Score:	**0** [1] AV:/AC:/Au:/C:/I:/A:
CVSS Temporal Score:	**0** E:ND/RL:ND/RC:ND
CVSS3 Base Score:	-
CVSS3 Temporal Score:	-
Severity:	**3**
QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/25/2018
User Modified:	-
Edited:	No

PCI Vuln: No
Ticket State:

First Detected: N/A

Last Detected: N/A

Times Detected:

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.
The Results section includes information on the remote access service that was found on the target.
Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:

Consequences vary by the type of attack.

SOLUTION:

Expose the remote access or remote management services only to the system administrators or intended users of the system.

RESULTS:

Service name: Remote Desktop on TCP port 3389.

Operating System Detected

PCI COMPLIANCE STATUS

PCI Severity: LOW

VULNERABILITY DETAILS

CVSS Base Score:	**0** [1]
CVSS Temporal Score:	**0**
CVSS3 Base Score:	-
CVSS3 Temporal Score:	-
Severity:	**2**
QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/21/2017
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: N/A

Last Detected: 11/26/2018 at 09:00:25 AM (GMT-0500)

Times Detected: 1

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.
1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:

Not applicable.

SOLUTION:

Not applicable.

RESULTS:

Operating System	Technique	ID
Windows 2008 Enterprise Server Service Pack 2	CIFS via TCP Port 445	
Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10	TCP/IP Fingerprint	U3414:593
Windows 2003/XP/Vista/2008/2012	MS-RPC Fingerprint	
Windows 2008/Vista	NTLMSSP	

Host Uptime Based on TCP TimeStamp Option

PCI COMPLIANCE STATUS

VULNERABILITY DETAILS

CVSS Base Score:	-
CVSS Temporal Score:	-
CVSS3 Base Score:	-
CVSS3 Temporal Score:	-
Severity:	**2**
QID:	82063
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/29/2007
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: N/A

Last Detected: N/A

Times Detected:

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:

N/A

SOLUTION:

N/A

RESULTS:

Based on TCP timestamps obtained via port 135, the host's uptime is 30 days, 21 hours, and 22 minutes.
The TCP timestamps from the host are in units of 10 milliseconds.

Windows Registry Pipe Access Level

PCI COMPLIANCE STATUS

PCI Severity: LOW

VULNERABILITY DETAILS

CVSS Base Score:	**0** [1]
CVSS Temporal Score:	**0**
CVSS3 Base Score:	-
CVSS3 Temporal Score:	-
Severity:	**2**
QID:	90194
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/16/2005
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: N/A

Last Detected: 11/26/2018 at 09:00:25 AM (GMT-0500)

Times Detected: 1

CVSS Environment:

Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:
Return code from remote access to the Windows registry pipe is displayed. The CIFS service accesses the Windows registry through a named pipe. Authentication to CIFS was successful, but it could not access the Registry named pipe if the error code is not 0.

IMPACT:
Vulnerabilities that require Windows registry access may not have been detected during the scan if the error code is not 0.

SOLUTION:
Error code 0x00 means the pipe access was successful. Other error codes (for eg: 0x0) denote unsuccessful access.

RESULTS:
Access to Remote Registry Service is denied, error: 0x0

Open DCE-RPC / MS-RPC Services List

PCI COMPLIANCE STATUS

VULNERABILITY DETAILS

CVSS Base Score: -
CVSS Temporal Score: -
CVSS3 Base Score: -
CVSS3 Temporal Score: -
Severity: **2** 
QID: 70022
Category: SMB / NETBIOS
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/06/2005
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: N/A
Last Detected: N/A
Times Detected:

CVSS Environment:
Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:
The following DCE-RPC / MS-RPC services are active on the remote host.

IMPACT:

N/A

SOLUTION:
Shut down any unknown or unused service on the list. In Windows, this is done in the "Services" Control Panel. In other environments, this usually requires editing a configuration file or start-up script.

If you have provided Windows Authentication credentials, the Microsoft
Registry service supporting the named pipe "\PIPE\winreg" must be present to allow CIFS to access the Registry.

RESULTS:

Description	Version	TCP Ports	UDP Ports	HTTP Ports	NetBIOS/CIFS Pipes
DCE Endpoint Mapper	3.0	135		593	
DCOM OXID Resolver	0.0	135		593	
DCOM Remote Activation	0.0	135		593	
DCOM System Activator	0.0	135		593	
Domain Name System	5.0	49156			
Message Queuing - QM2QM V1	1.0	2105, 2103, 2107, 49157			
Message Queuing - QMRT V1	1.0	2105, 2103, 2107, 49157			
Message Queuing - QMRT V2	1.0	2105, 2103, 2107, 49157			
Message Queuing - RemoteRead V1	1.0	2105, 2103, 2107, 49157			
Microsoft Scheduler Control Service	1.0				\PIPE\atsvc
Microsoft Security Account Manager	1.0	49153			\pipe\lsass
Microsoft Service Control Service	2.0	49159			
Microsoft Task Scheduler	1.0				\PIPE\atsvc
(Unknown Service)	1.0	135		593	
(Unknown Service)	0.0	135		593	
(Unknown Service)	2.0	135		593	
(Unknown Service)	1.0	49152			\PIPE\InitShutdown
(Unknown Service)	1.0				\PIPE\InitShutdown
KeyIso	1.0	49153			\pipe\lsass
Impl friendly name	1.0	49155			\pipe\lsass, \PIPE\srvsvc, \PIPE\atsvc
Event log TCPIP	1.0	49154			\pipe\eventlog
(Unknown Service)	1.0	49155			\PIPE\srvsvc, \PIPE\atsvc
IAS RPC server	1.0	49155			\PIPE\atsvc
IKE/Authip API	1.0	49155			\PIPE\atsvc
(Unknown Service)	1.0	49155			\PIPE\atsvc
(Unknown Service)	1.0	49158			
TsProxyMgmt	1.0			3388	
TsProxy	1.3			3388	
Unimodem LRPC Endpoint	1.0				\pipe\tapsrv
(Unknown Service)	1.0	5040			

Firewall Detected

PCI COMPLIANCE STATUS

VULNERABILITY DETAILS

CVSS Base Score: -
CVSS Temporal Score: -
CVSS3 Base Score: -
CVSS3 Temporal Score: -

Severity:	**1**
QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/16/2001
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: N/A

Last Detected: N/A

Times Detected:

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULTS:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 443, 1.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-3,5,7,9,11,13,15,17-25,27,29,31,33,35,37-39,41-134,136-223,242-246,
256-265,280-282,309,311,318,322-325,344-351,363,369-444,446-581,587,592,
598,600,606-620,624,627,631,633-637,666-674,700,704-705,707,709-711,729-731,
740-742,744,747-754,758-765,767,769-777,780-783,786,799-801,860,873,886-888,
900-901,911,950,954-955,990-993,995-1001,1008,1010-1011,1015,1023-1100,
1109-1112,1114,1123,1155,1167,1170,1207,1212,1214,1220-1222,1234-1236,
1241,1243,1245,1248,1269,1313-1314,1337,1344-1625,1636-1705,1707-1774,
1776-1815,1818-1824,1900-1909,1911-1920,1944-1951,1973,1981,1985-1999,
2001-2028,2030,2032-2036,2038,2040-2049,2053,2065,2067,2080,2097,2100, and more.
We have omitted from this list 704 higher ports to keep the report size manageable.

NetBIOS Host Name

PCI COMPLIANCE STATUS

VULNERABILITY DETAILS

CVSS Base Score:	-
CVSS Temporal Score:	-
CVSS3 Base Score:	-
CVSS3 Temporal Score:	-
Severity:	**1**
QID:	82044
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-

Bugtraq ID: -
Service Modified: 01/20/2005
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: N/A
Last Detected: 11/26/2018 at 09:00:25 AM (GMT-0500)
Times Detected: 1

CVSS Environment:
- Asset Group: -
- Collateral Damage Potential: -
- Target Distribution: -
- Confidentiality Requirement: -
- Integrity Requirement: -
- Availability Requirement: -

THREAT:
The NetBIOS host name of this computer has been detected.

IMPACT:
N/A

SOLUTION:
N/A

RESULTS:
COM-2K8-32-86

Windows Authentication Method

PCI COMPLIANCE STATUS

PCI Severity: LOW

VULNERABILITY DETAILS

CVSS Base Score: **0** [1]
CVSS Temporal Score: **0**
CVSS3 Base Score: -
CVSS3 Temporal Score: -
Severity: **1**
QID: 70028
Category: SMB / NETBIOS
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 12/09/2008
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: N/A
Last Detected: N/A
Times Detected:

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Windows authentication was performed. The Results section in your detailed results includes a list of authentication credentials used.
The service also attempts to authenticate using common credentials. You should verify that the credentials used for successful authentication were those that were provided in the Windows authentication record. User-provided credentials failed if the discovery method shows "Unable to log in using credentials provided by user, fallback to NULL session". If this is the case, verify that the credentials specified in the Windows authentication record are valid for this host.

IMPACT:

N/A

SOLUTION:

N/A

RESULTS:

User Name	(none)
Domain	(none)
Authentication Scheme	NULL session
Security	User-based
SMBv1 Signing	Enabled
Discovery Method	Unable to log in using credentials provided by user, fallback to NULL session
CIFS Signing	default
CIFS Version	SMB v2.0.2

Open TCP Services List

PCI COMPLIANCE STATUS

PCI Severity: LOW

VULNERABILITY DETAILS

CVSS Base Score:	**0** [1] AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Temporal Score:	**0** E:U/RL:W/RC:UC
CVSS3 Base Score:	-
CVSS3 Temporal Score:	-
Severity:	**1**
QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/15/2009
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: N/A

Last Detected: 11/26/2018 at 09:00:25 AM (GMT-0500)

Times Detected: 1

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
135	msrpc-epmap	epmap DCE endpoint resolution	DCERPC Endpoint Mapper	
445	microsoft-ds	Microsoft-DS	microsoft-ds	
593	http-rpc-epmap	HTTP RPC Ep Map	msrpc-over-http	
3389	ms-wbt-server	MS WBT Server	win remote desktop over ssl	

Windows Authentication Failed

PCI COMPLIANCE STATUS

PCI Severity: LOW

VULNERABILITY DETAILS

CVSS Base Score:	**0** [1]
CVSS Temporal Score:	**0**
CVSS3 Base Score:	-
CVSS3 Temporal Score:	-
Severity:	**1**
QID:	105015
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/12/2008
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: N/A

Last Detected: N/A

Times Detected:

CVSS Environment:

Asset Group:	-

Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:
Windows authentication was enabled during the scan but login attempts for this host failed, using the authentication credentials specified in the Windows authentication record.

IMPACT:
For a vulnerability scan, vulnerabilities that require Windows authentication may not be detected. For a compliance scan, the assessment phase does not occur and compliance data is not collected for the host.

SOLUTION:
Verify that the authentication credentials defined in the Windows authentication record are valid for this host. Also verify that the host permits network login attempts. For domain level authentication, verify that the host is a member of the specified domain.
For Windows XP, make sure that the "use simple file sharing" option is cleared. This can be done through the "view" tab sheet of the "folder options" GUI, which can be invoked from the Control Panel. The machine requires a reboot for new settings to take effect.
The Result section in your detailed results shows the name of the authentication record that failed. Note that Windows authentication may fail for many reasons. Thus, the absence of this QID does not necessarily indicate that authentication was successful.

RESULTS:

Authentication Record	User Name	Cause
Qualys - QA Lab - Windows	administrator	Login error

Traceroute

PCI COMPLIANCE STATUS

VULNERABILITY DETAILS

CVSS Base Score: -
CVSS Temporal Score: -
CVSS3 Base Score: -
CVSS3 Temporal Score: -
Severity: **1** 
QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/09/2003
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: N/A
Last Detected: N/A
Times Detected:

CVSS Environment:
Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -

Availability Requirement: -

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULTS:

Hops	IP	Round Trip Time	Probe
1	10.10.22.2	0.81ms	ICMP
2	10.10.0.10	0.50ms	ICMP
3	10.10.32.86	0.45ms	TCP

Degree of Randomness of TCP Initial Sequence Numbers

PCI COMPLIANCE STATUS

VULNERABILITY DETAILS

CVSS Base Score: -
CVSS Temporal Score: -
CVSS3 Base Score: -
CVSS3 Temporal Score: -
Severity: **1**
QID: 82045
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 11/19/2004
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: N/A
Last Detected: N/A
Times Detected:

CVSS Environment:
Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:
N/A

SOLUTION:
N/A

RESULTS:

Average change between subsequent TCP initial sequence numbers is 1001276964 with a standard deviation of 531835509. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(7022 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

Microsoft Windows Network Level Authentication Disabled

PCI COMPLIANCE STATUS

PCI Severity: LOW

VULNERABILITY DETAILS

CVSS Base Score:	**0** [1] AV:/AC:/Au:/C:/I:/A:
CVSS Temporal Score:	**0** E:ND/RL:ND/RC:ND
CVSS3 Base Score:	-
CVSS3 Temporal Score:	-
Severity:	**1**
QID:	90788
Category:	Windows
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/01/2013
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: N/A

Last Detected: N/A

Times Detected:

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Microsoft Windows Network Level Authentication (NLA) is an authentication method that enhances the security of a Remote Desktop Session Host server by requiring the user to be authenticated before a session is created.
The registry key for the Network Level Authentication (NLA) is disabled.
Network Level Authentication is supported on Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2

IMPACT:

Enabling NLA can help protect the remote computer from malicious users and malicious software attacks.

SOLUTION:

See Microsoft Knowledge Base Article 2671387 (http://support.microsoft.com/kb/2671387) to use the automated Microsoft Fix it solution to enable this feature.
As a precaution, always test in a QA or rehearsal environment before rolling out to production.
Note: Client computers that do not support Credential Security Support Provider (CredSSP) protocol will not be able to access servers protected with Network Level Authentication. Windows XP does not support the CredSSP protocol by default.

RESULTS:

QID: 90788 detected on port 3389 over TCP.

IP ID Values Randomness

PCI COMPLIANCE STATUS

VULNERABILITY DETAILS

CVSS Base Score:	-
CVSS Temporal Score:	-
CVSS3 Base Score:	-
CVSS3 Temporal Score:	-
Severity:	**1**
QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: N/A

Last Detected: N/A

Times Detected:

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:

N/A

SOLUTION:

N/A

RESULTS:

IP ID changes observed (network order) for port 135: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Duration: 9 milli seconds

DNS Host Name

PCI COMPLIANCE STATUS

VULNERABILITY DETAILS

CVSS Base Score: -
CVSS Temporal Score: -
CVSS3 Base Score: -
CVSS3 Temporal Score: -
Severity: **1**
QID: 6

Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/04/2018
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: N/A
Last Detected: 11/26/2018 at 09:00:25 AM (GMT-0500)
Times Detected: 1

CVSS Environment:
Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

RESULTS:

IP address	Host name
10.10.32.86	No registered hostname

Host Scan Time

PCI COMPLIANCE STATUS

VULNERABILITY DETAILS

CVSS Base Score: -
CVSS Temporal Score: -
CVSS3 Base Score: -
CVSS3 Temporal Score: -
Severity: **1**
QID: 45038

Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: N/A

Last Detected: 11/26/2018 at 09:00:25 AM (GMT-0500)

Times Detected: 1

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:

N/A

SOLUTION:

N/A

RESULTS:

Scan duration: 1177 seconds

Start time: Mon, Nov 26 2018, 13:40:48 GMT

End time: Mon, Nov 26 2018, 14:00:25 GMT

Host Names Found

PCI COMPLIANCE STATUS

VULNERABILITY DETAILS

CVSS Base Score:	-
CVSS Temporal Score:	-
CVSS3 Base Score:	-
CVSS3 Temporal Score:	-
Severity:	**1** 
QID:	45039
Category:	Information gathering
CVE ID:	-

Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/14/2005
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: N/A
Last Detected: 11/26/2018 at 09:00:25 AM (GMT-0500)
Times Detected: 1

CVSS Environment:
- Asset Group: -
- Collateral Damage Potential: -
- Target Distribution: -
- Confidentiality Requirement: -
- Integrity Requirement: -
- Availability Requirement: -

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

RESULTS:

Host Name	Source
com-2k8-32-86	NTLM DNS
COM-2K8-32-86	NTLM NetBIOS

TLS Secure Renegotiation Extension Support Information — port 3389/tcp

PCI COMPLIANCE STATUS

PCI Severity: LOW

VULNERABILITY DETAILS

CVSS Base Score: **0** [1] AV:/AC:/Au:/C:/I:/A:
CVSS Temporal Score: **0** E:ND/RL:ND/RC:ND
CVSS3 Base Score: -
CVSS3 Temporal Score: -
Severity: **1**
QID: 42350
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 03/21/2016
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: N/A

Last Detected: N/A

Times Detected:

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:

N/A

SOLUTION:

N/A

RESULTS:

TLS Secure Renegotiation Extension Status: supported.

SSL Certificate - Information port 3389/tcp

PCI COMPLIANCE STATUS

VULNERABILITY DETAILS

CVSS Base Score:	-
CVSS Temporal Score:	-
CVSS3 Base Score:	-
CVSS3 Temporal Score:	-
Severity:	**1**
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/23/2003
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: N/A

Last Detected: N/A

Times Detected:

CVSS Environment:

Asset Group:	-

Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	06:a7:c6:ce:9c:3b:53:af:45:de:05:9d:9f:b7:f3:f8
(0)Signature Algorithm	sha1WithRSAEncryption
(0)ISSUER NAME	
commonName	com-2k8-32-86
(0)SUBJECT NAME	
commonName	com-2k8-32-86
(0)Valid From	Sep 14 06:17:19 2016 GMT
(0)Valid Till	Mar 16 06:17:19 2017 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:8b:8a:98:c1:ce:52:ea:aa:0d:c7:cc:c7:7a:b2:
(0)	66:75:6a:ff:f7:11:23:f3:4d:58:f0:95:32:61:af:
(0)	35:cc:a0:e5:04:47:0f:b9:9d:6d:96:a6:d0:31:cc:
(0)	24:59:2f:33:7b:34:66:7c:6d:63:6c:6a:bf:3a:fc:
(0)	b1:4b:64:83:04:4b:01:b3:ff:4d:69:06:86:20:c1:
(0)	a5:ae:5a:de:8c:40:3e:95:82:c5:c1:fe:db:4c:4b:
(0)	f9:0a:24:95:a7:d8:5f:19:83:c8:a6:a1:ed:d7:0b:
(0)	ef:a9:1a:ab:df:2b:77:2e:ee:14:49:20:ed:74:66:
(0)	6d:08:c7:4b:ed:eb:a9:2c:af:ee:4a:6d:3c:00:13:
(0)	fb:7e:c5:7e:e7:11:69:67:2e:77:1c:1e:a0:6b:34:
(0)	41:d2:54:82:94:55:c4:fd:29:87:99:2a:1b:08:3e:
(0)	85:0d:46:a1:26:7b:3f:1e:5d:df:08:29:40:65:5a:
(0)	f8:95:87:57:6e:58:d1:75:ff:ad:c0:70:c3:2c:4a:
(0)	8a:e9:42:b9:b3:ed:dc:f5:5f:52:38:39:53:7a:82:
(0)	76:a3:67:4f:66:dd:91:fd:61:54:37:4f:23:1f:4f:
(0)	55:91:03:74:19:ce:8c:79:38:a7:bf:55:87:8a:35:
(0)	5d:d5:2a:00:1f:53:81:09:4b:0f:bc:ad:19:3a:b6:
(0)	9d:61
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Extended Key Usage	TLS Web Server Authentication
(0)X509v3 Key Usage	Key Encipherment, Data Encipherment
(0)Signature	(256 octets)
(0)	5f:b5:4d:7b:75:8f:cf:a4:6c:25:4a:41:e1:91:aa:5b
(0)	4b:21:31:85:cb:d7:87:bd:58:1e:8a:24:15:f2:32:28
(0)	8a:6d:18:4f:ea:2a:7d:97:39:13:3d:4b:d5:cd:d3:4e
(0)	25:37:ce:0d:e8:48:96:6b:f7:91:80:f0:2d:58:93:8e
(0)	bd:89:de:7b:86:b8:4e:32:53:ab:af:3f:b3:c1:32:e4
(0)	4d:5f:d5:96:3a:cd:09:55:87:d1:d5:ea:45:fa:db:82
(0)	bb:79:2a:14:f8:bf:96:28:10:44:16:ab:a0:86:9a:25
(0)	95:6b:3f:96:0c:bb:c3:c4:75:c5:c0:71:f3:77:e9:5d
(0)	d3:21:64:39:76:9e:3b:cc:a7:2e:da:29:d2:f2:ad:63
(0)	ec:11:9c:7e:80:08:9c:be:fe:04:86:d5:e0:d0:31:f2

(0)	f5:a3:10:b5:ef:60:b0:3b:be:54:8b:7e:8a:88:f4:f6
(0)	28:17:f1:c2:22:db:f7:c5:a1:e7:d3:18:10:b7:b2:46
(0)	ac:a9:ba:56:b5:54:ce:e9:a8:d2:15:be:e3:4e:37:72
(0)	02:76:38:a6:73:28:5b:0e:27:f1:b4:7f:e4:b5:af:d5
(0)	60:f9:b6:5b:57:29:3a:8a:4f:41:91:18:bd:ff:5d:f7
(0)	95:f3:78:5e:6d:03:82:27:36:6f:16:aa:3d:21:80:9e

SSL Certificate will expire within next six months port 3389/tcp

PCI COMPLIANCE STATUS

PCI Severity: LOW

VULNERABILITY DETAILS

CVSS Base Score: **0** [1] AV:/AC:/Au:/C:/I:/A:
CVSS Temporal Score: **0** E:ND/RL:ND/RC:ND
CVSS3 Base Score: -
CVSS3 Temporal Score: -
Severity: **1**
QID: 38600
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/29/2016
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: N/A
Last Detected: N/A
Times Detected:

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:
Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

IMPACT:
Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

SOLUTION:
Contact the certificate authority that signed your certificate to arrange for a renewal.

RESULTS:
Certificate #0 CN=com-2k8-32-86 The certificate will expire within six months: Mar 16 06:17:19 2017 GMT

SSL/TLS invalid protocol version tolerance port 3389/tcp

PCI COMPLIANCE STATUS

PCI Severity: LOW

VULNERABILITY DETAILS

CVSS Base Score: **0** [1] AV:/AC:/Au:/C:/I:/A:
CVSS Temporal Score: **0** E:ND/RL:ND/RC:ND
CVSS3 Base Score: -
CVSS3 Temporal Score: -
Severity: **1**
QID: 38597
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/29/2016
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: N/A
Last Detected: N/A
Times Detected:

CVSS Environment:
- Asset Group: -
- Collateral Damage Potential: -
- Target Distribution: -
- Confidentiality Requirement: -
- Integrity Requirement: -
- Availability Requirement: -

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

RESULTS:

my version	target version
0304	0301
0399	0301
0400	0301
0499	0301

SSL Server Information Retrieval port 3389/tcp

PCI COMPLIANCE STATUS

VULNERABILITY DETAILS

CVSS Base Score: -
CVSS Temporal Score: -
CVSS3 Base Score: -
CVSS3 Temporal Score: -
Severity: **1**
QID: 38116

Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/24/2016
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: N/A
Last Detected: N/A
Times Detected:

CVSS Environment:

Asset Group: -
Collateral Damage Potential: -
Target Distribution: -
Confidentiality Requirement: -
Integrity Requirement: -
Availability Requirement: -

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS ENABLED					
TLSv1	COMPRESSION METHOD	None			
RC4-MD5	RSA	RSA	MD5	RC4(128)	MEDIUM
RC4-SHA	RSA	RSA	SHA1	RC4(128)	MEDIUM
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.1 PROTOCOL IS DISABLED					
TLSv1.2 PROTOCOL IS DISABLED					

PCI COMPLIANCE STATUS

VULNERABILITY DETAILS

CVSS Base Score:	-
CVSS Temporal Score:	-
CVSS3 Base Score:	-
CVSS3 Temporal Score:	-
Severity:	**1**
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/16/2004
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: N/A

Last Detected: N/A

Times Detected:

CVSS Environment:

Asset Group:	-
Collateral Damage Potential:	-
Target Distribution:	-
Confidentiality Requirement:	-
Integrity Requirement:	-
Availability Requirement:	-

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

RESULTS:

TLSv1 session caching is disabled on the target.

Appendix

Report Filters

Status:	New, Active, Re-Opened
Display non-running kernels:	Off
Exclude non-running kernels:	Off
Exclude non-running services:	Off
Exclude QIDs not exploitable due to configuration:	Off
Vulnerabilities:	State:Active, Disabled
Potential Vulnerabilities:	State:Active, Disabled
Information Gathered:	State:Active, Disabled
Included Operating Systems:	All Operating Systems

Report Legend

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.

Severity	Level	Description
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.

Footnotes

This footnote indicates that the CVSS Base score that is displayed for the vulnerability is not supplied by NIST. When the service looked up the latest NIST score for the vulnerability, as published in the National Vulnerability Database (NVD), NIST either listed the CVSS Base score as 0 or did not provide a score in the NVD. In this case, the service determined that the severity of the vulnerability warranted a higher CVSS Base score. The score provided by the service is displayed.

This report was generated with an evaluation version of