Bites-PenTesting

Penetration Test Report

Client: *REMOVED*

Date of test: 25-03-2015 – 27-03-2015

Due to the removal of sensitive information the formatting of this report has become slightly off.

DISCLAIMER

This report is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this disclaimer is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this document is strictly prohibited. If you received this document in error, please notify us immediately by telephone and return the original document to us at the post address below.

Thank you

Contents

Vulnerabilities by host

Introduction to the penetration test

The aim of this penetration test is to help the administrator of the company to secure the network. Although this report contains technical terms, it has been written so that a non-initiated reader with a basic knowledge of computing would understand. This test was carried out remotely via VNC to a Linux virtual machine to enable an internal test to be carried out.

Some definitions

- Hacker: word given by the masse media to define what we will more accurately call attacker or intruder in this report.

- Vulnerability: a bug in computer program that may be abused to gain privileges on a computer.

- Exploit: a program or strategy to exploit a vulnerability. Depending on the vulnerability, an exploit may be either local, in which a previous “local” access to the target computer is required prior gain higher privileges, or remote where the exploit can be run without this prerequisite.

- Rootkit: a set of programs replacing the tools, that an administrator would generally use to detect the presence of an intruder, by modified versions detecting everything but the presence and activities of the intruder, thus making the administrator confident that the system is free of any intrusions.

Motivation of an attacker

There are mainly three reasons why someone might want to penetrate your network.

• Information theft: to steal valuable information of your business such as contracts, documents or e-mail communication. In other words, information that, for example, competitors may like to know.

• Identity theft: by using your network as relay to attack other net- works, an attacker can mask his identity.

• Challenge to overcome: to most attackers, your network represents a challenge that must be conquered or a way to prove their superior intelligence and technical skills.

Understanding the psychology of an attacker helps considering why your network is at risk whenever it is connected to the Internet and how to protect it. Indeed, whatever the final motivation really is, gaining access to a network always remains a challenge for an attacker. Though intruding a network is rewarding for his ego, failing to gain the access brings a high level of frustration. An attacker, usually, doesn't give up easily and will try, again and again, by any means, to get all kind of information that might be useful to detect weaknesses and mount attacks.

Therefore, while performing the penetration test, we have been through the same stages, as an attacker would have, even though our strategy or tools might be slightly differ.

Intro

The penetration test has been limited to the boundaries set in the conversation before I begun the test. No vulnerability was exploited and Denial of Service techniques were not used although a Denial of Service vulnerability was found by looking at TCP responses from one packet sent to your servers. This test was rather slow as the VNC connection was lagging a lot, this effected productivity of the tester.

192.168.0.1

Summary

Critical	High	Medium	Low
0	2	2	2

High (7.5)		SNMP Agent Default Community Names

Synopsis:

The community names of the remote SNMP server can be guessed.

Description:

It is possible to obtain the default community names 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).

Solution:

Disable the SNMP service on the remote host if you do not use it, filter incoming UDP packets going to this port, or change the default community string.

Risk factor:

High / CVSS Base Score: 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS Temporal Score: 6.2
(CVSS2#E:F/RL:OF/RC:C)
Public Exploit Available: true

High (7.5)		SNMP Agent Default Community Name

Synopsis:
The community name of the remote SNMP server can be guessed.

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).
Solution:

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.

Risk factor:

High / CVSS Base Score: 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS Temporal Score: 7.1
(CVSS2#E:F/RL:U/RC:ND)

Medium (5.0)		DNS Server Cache Snooping Remote Information Disclosure

Synopsis:
The remote DNS server is vulnerable to cache snooping attacks.

Description:
The remote DNS server responds to queries for third-party domains that do not have the recursion bit set.

This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

For instance, if an attacker was interested in whether your company utilises the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.

Note: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.

See also :

http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf

Solution:
Contact the vendor of the DNS software for a fix.

Risk factor:
Medium / CVSS Base Score: 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Medium (5.0)		SNMP 'GETBULK' Reflection DDoS

Synopsis :
The remote SNMP daemon is affected by a vulnerability that allows a reflected distributed denial of service attack.

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.

Solution :
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.

Risk factor :
Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

Low (3.3)		DHCP Server Detection

Synopsis :
The remote DHCP server may expose information about the associated network.

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.

Solution :
Apply filtering to keep this information off the network and remove any options that are not in use.

Risk factor :
Low / CVSS Base Score : 3.3
(CVSS2#AV:A/AC:L/Au:N/C:P/I:N/A:N)

Low (3.3)		Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)

Synopsis :
The remote host appears to leak memory in network packets.

Description :
The remote host uses a network device driver that pads ethernet frames with data which vary from one packet to another, likely taken from kernel memory, system memory allocated to the device driver, or a hardware buffer on its network interface card.

Known as 'Etherleak', this information disclosure vulnerability may allow an attacker to collect sensitive information from the affected host provided he is on the same physical subnet as that host.

Solution :
Contact the network device driver's vendor for a fix.

Risk factor :
Low / CVSS Base Score : 3.3
(CVSS2#AV:A/AC:L/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 2.9
(CVSS2#E:ND/RL:OF/RC:C)

192.168.0.2

Summary

Critical	High	Medium	Low
0	0	13	4

Medium (6.4)		SSL Certificate Cannot Be Trusted

Synopsis :
The SSL certificate for this service cannot be trusted.

Description :
The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

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 unrecognised, 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 is not recognise.

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.

Solution :
Purchase or generate a proper certificate for this service.

Risk factor :

Medium / CVSS Base Score : 6.4

(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Medium (6.4)		SSL Self-Signed Certificate

Synopsis :
The SSL certificate chain for this service ends in an unrecognised self-signed certificate.

Description :
The X.509 certificate chain for this service is not signed by a recognised 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 unrecognised certificate authority.

Solution :
Purchase or generate a proper certificate for this service.

Risk factor :
Medium / CVSS Base Score : 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Medium (5.8)		SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

Synopsis :
The remote service allows insecure renegotiation of TLS / SSL connections.

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.

See also :
http://www.ietf.org/mail-archive/web/tls/current/msg03948.html
http://www.g-sec.lu/practicaltls.pdf

http://tools.ietf.org/html/rfc5746

Solution :
Contact the vendor for specific patch information.

Risk factor :
Medium / CVSS Base Score : 5.8
(CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)
CVSS Temporal Score : 5.0
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

Medium (5.1)		Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle

Synopsis :
It may be possible to get access to the remote host.

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.

See also :
http://www.oxid.it/downloads/rdp-gbu.pdfhttp://technet.microsoft.com/en-us/library/cc782610.aspx

Solution :
- 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.

Risk factor :
Medium / CVSS Base Score : 5.1
(CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 4.6
(CVSS2#E:F/RL:W/RC:ND)
Public Exploit Available : true

Medium (5.0)		DNS Server Cache Snooping Remote Information Disclosure

Synopsis :
The remote DNS server is vulnerable to cache snooping attacks.

Description :
The remote DNS server responds to queries for third-party domains that does not have the recursion bit set.

This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.

Note: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.

See also :
http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf

Solution :
Contact the vendor of the DNS software for a fix.

Risk factor :

Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Medium (5.0)		SSL Certificate Expiry

Synopsis :
The remote server's SSL certificate has already expired.

Description :
This script checks expiry dates of certificates associated with SSL-enabled services on the target and reports whether any have already expired.

Solution :
Purchase or generate a new SSL certificate to replace the existing one.

Risk factor:

edium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Medium (5.0)		SSL Version 2 and 3 Protocol Detection

Synopsis :
The remote service encrypts traffic using a protocol with known weaknesses.

Description :
The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0, which reportedly suffer from several cryptographic flaws. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

NIST has determined SSL v3.0 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 SSCA’s definition of strong cryptography.

See also :

http://www.schneier.com/paper-ssl.pdf
http://support.microsoft.com/kb/187498

http://www.linux4beginners.info/node/disable-sslv2
https://www.openssl.org/~bodo/ssl-poodle.pdf

Solution :
Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.0 or higher instead.

Risk factor :
Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Medium (5.0)		SSL Certificate with Wrong Hostname

Synopsis :
The SSL certificate for this service is for a different host.

Description :
The commonName (CN) of the SSL certificate presented on this service
is for a different machine.

Solution :
Purchase or generate a proper certificate for this service.

Risk factor :
Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Medium (4.3)		SSL Weak Cipher Suites Supported

Synopsis :
The remote service supports the use of weak SSL ciphers.

Description :
The remote host supports the use of SSL ciphers that offer weak
encryption.

Note: This is considerably easier to exploit if the attacker is on the
same physical network.

See also :
http://www.openssl.org/docs/apps/ciphers.html

Solution :

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Medium (4.3)		Terminal Services Encryption Level is Medium or Low

Synopsis :
The remote host is using weak cryptography.

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.

Solution :
Change RDP encryption level to one of :

3. High

4. FIPS Compliant

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Medium (4.3)		Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Synopsis :
The remote Terminal Services doesn't use Network Level Authentication only.

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.

See also :
http://technet.microsoft.com/en-us/library/cc732713.aspx

Solution :

Enable Network Level Authentication (NLA) on the remote RDP server. This is
generally done on the 'Remote' tab of the 'System' settings on Windows.

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Medium (4.3)		SSL/TLS Protocol Initialization Vector Implementation Information Disclosure

Synopsis :
It may be possible to obtain sensitive information from the remote
host with SSL/TLS-enabled services.

Description :
Vulnerability exists in SSL 3.0 and TLS 1.0 that could allow
information disclosure if an attacker intercepts encrypted traffic
served from an affected system.

TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are
not affected.

This script tries to establish an SSL/TLS remote connection using an
affected SSL version and cipher suite, and then solicits return data.
If returned application data is not fragmented with an empty or
one-byte record, it is likely vulnerable.

OpenSSL uses empty fragments as a countermeasure unless the
'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when
OpenSSL
is initialized.

Microsoft implemented one-byte fragments as a countermeasure, and the
setting can be controlled via the registry key
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders
\SCHANNEL\SendExtraRecord.

Therefore, if multiple applications use the same SSL/TLS implementation, some may be vulnerable while others may not, depending on whether or not a countermeasure has been enabled.

Note that this script detects the vulnerability in the SSLv3/TLSv1 protocol implemented in the server. It does not detect the BEAST attack where it exploits the vulnerability at HTTPS client-side (i.e., Internet browser). The detection at server-side does not necessarily mean your server is vulnerable to the BEAST attack because the attack exploits the vulnerability at client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure.

See also :
http://www.openssl.org/~bodo/tls-cbc.txt
http://vnhacker.blogspot.com/2011/09/beast.html
http://technet.microsoft.com/en-us/security/bulletin/ms12-006
http://support.microsoft.com/kb/2643584
http://blogs.msdn.com/b/kaushal/archive/2012/01/21/fixing-the-beast.aspx

Solution :
Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported. Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available.

Note that additional configuration may be required after the installation of the MS12-006 security update in order to enable the split-record countermeasure. See Microsoft KB2643584 for details.

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 3.7
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

Medium (4.3)		SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis :
It is possible to obtain sensitive information from the remote host

with SSL/TLS-enabled services.

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 vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See also :
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

Solution :
Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 3.7
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

Low (2.6)	30218	Terminal Services Encryption Level is not

FIPS-140 Compliant

Synopsis :
The remote host is not FIPS-140 compliant.

Description :
The encryption setting used by the remote Terminal Services service
is not FIPS-140 compliant.

Solution :
Change RDP encryption level to :

4. FIPS Compliant

Risk factor :
Low / CVSS Base Score : 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Low (2.6)

SSL Anonymous Cipher Suites Supported

Synopsis :
The remote service supports the use of anonymous SSL ciphers.

Description :
The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See also :
http://www.openssl.org/docs/apps/ciphers.html

Solution :
Reconfigure the affected application if possible to avoid use of weak ciphers.

Risk factor :

Low / CVSS Base Score : 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score : 2.3
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

Low (2.6)		SSL RC4 Cipher Suites Supported

Synopsis :
The remote service supports the use of the RC4 cipher.

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.

See also :
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/

Solution :
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.

Risk factor :
Low / CVSS Base Score : 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 2.3
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : false

Low		SSL Certificate Chain Contains RSA Keys L

Synopsis :
The X.509 certificate chain used by this service contains certificates

with RSA keys shorter than 2048 bits.

Description :
At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.

Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

See also :

https://www.cabforum.org/Baseline_Requirements_V1.pdf

Solution :
Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Risk factor :
Low

192.168.0.3

Summary

Critical	High	Medium	Low
0	7	12	3

High (9.4)		OpenSSL Heartbeat Information Disclosure (Heartbleed)

Synopsis :
The remote service is affected by an information disclosure vulnerability.

Description :
Based on its response to a TLS request with a specially crafted heartbeat message (RFC 6520), the remote service appears to be affected by an out-of-bounds read flaw.

This flaw could allow a remote attacker to read the contents of up to 64KB of server memory, potentially exposing passwords, private keys, and other sensitive data.

See also :
http://heartbleed.com/
http://eprint.iacr.org/2014/140
http://www.openssl.org/news/vulnerabilities.html#2014-0160

Solution :
Upgrade to OpenSSL 1.0.1g or later.

Alternatively, recompile OpenSSL with the '-DOPENSSL_NO_HEARTBEATS' flag to disable the vulnerable functionality.

Risk factor :
High / CVSS Base Score : 9.4
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:N)
CVSS Temporal Score : 8.2
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

High (9.4)		HP System Management Homepage OpenSSL Multiple Vulnerabilities

Synopsis :
The remote web server is affected by multiple vulnerabilities.

Description :
According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server has an

implementation of the OpenSSL library affected by the following issues :

- An error exists in the 'ssl3_take_mac' function in the file 'ssl/s3_both.c' related to handling TLS handshake traffic that could lead to denial of service attacks. (CVE-2013-4353)

- An error exists in the 'ssl_get_algorithm2' function in the file 'ssl/s3_lib.c' related to handling TLS 1.2 traffic that could lead to denial of service attacks. (CVE-2013-6449)

- An error exists related to the handling of DTLS retransmission processes that could lead to denial of service attacks. (CVE-2013-6450)

- An out-of-bounds read error, known as the 'Heartbleed Bug', exists related to handling TLS heartbeat extensions that could allow an attacker to obtain sensitive information such as primary key material, secondary key material, and other protected content. (CVE-2014-0160)

See also :
http://www.heartbleed.com/
http://www.securityfocus.com/archive/1/532007/30/0/threaded
http://www.securityfocus.com/archive/1/532095/30/0/threaded

Solution :
Upgrade to HP System Management Homepage 7.2.3.1 (Linux or Windows) / 7.3.2.1(B) (Windows) or later.

Risk factor :
High / CVSS Base Score : 9.4
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:N)
CVSS Temporal Score : 8.2
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

High (9.3)		HP System Management Homepage < 7.2.4.1 / 7.3.3.1 OpenSSL Multiple

Synopsis :

The remote web server is affected by multiple vulnerabilities.

Description :

According to the web server's banner, the version of HP System
Management Homepage (SMH) hosted on the remote web server has an
implementation of the OpenSSL library affected by the following
vulnerabilities :

- An error exists in the function 'ssl3_read_bytes'
that could allow data to be injected into other
sessions or allow denial of service attacks. Note
this issue is only exploitable if
'SSL_MODE_RELEASE_BUFFERS' is enabled. (CVE-2010-5298)

- An error exists related to the implementation of the
Elliptic Curve Digital Signature Algorithm (ECDSA) that
could allow nonce disclosure via the 'FLUSH+RELOAD'
cache side-channel attack. (CVE-2014-0076)

- A buffer overflow error exists related to invalid DTLS
fragment handling that could lead to execution of
arbitrary code. Note this issue only affects OpenSSL
when used as a DTLS client or server. (CVE-2014-0195)

- An error exists in the function 'do_ssl3_write' that
could allow a NULL pointer to be dereferenced leading
to denial of service attacks. Note this issue is
exploitable only if 'SSL_MODE_RELEASE_BUFFERS' is
enabled. (CVE-2014-0198)

- An error exists related to DTLS handshake handling that
could lead to denial of service attacks. Note this
issue only affects OpenSSL when used as a DTLS client.
(CVE-2014-0221)

- An unspecified error exists that could allow an
attacker to cause usage of weak keying material
leading to simplified man-in-the-middle attacks.
(CVE-2014-0224)

- An unspecified error exists related to anonymous ECDH
ciphersuites that could allow denial of service

attacks. Note this issue only affects OpenSSL TLS clients. (CVE-2014-3470)

See also :
http://www.securityfocus.com/archive/1/532538/30/0/threaded
http://www.securityfocus.com/archive/1/532642/30/0/threaded
http://www.openssl.org/news/vulnerabilities.html#CVE-2010-5298
http://www.openssl.org/news/vulnerabilities.html#2014-0076
http://www.openssl.org/news/vulnerabilities.html#CVE-2014-0198
http://www.openssl.org/news/vulnerabilities.html#CVE-2014-0221
http://www.openssl.org/news/vulnerabilities.html#CVE-2014-0224
http://www.openssl.org/news/vulnerabilities.html#CVE-2014-3470
http://www.openssl.org/news/secadv_20140605.txt

Solution :
Upgrade to HP System Management Homepage 7.2.4.1 (Windows 2003) / 7.3.3.1 (Linux or Windows) or later.

Note that version 7.3.3.1 for Linux x86 still contains OpenSSL v1.0.0d.

Ensure that any products with which such an install might communicate have been updated to the latest versions to not be affected by the vulnerability covered by CVE-2014-0224.

Risk factor :
High / CVSS Base Score : 9.3
(CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)
CVSS Temporal Score : 8.1
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

High (9.3)		OpenSSL 'ChangeCipherSpec' MiTM

Synopsis :
The remote host is affected by a vulnerability that could allow sensitive data to be decrypted.

Description :
The OpenSSL service on the remote host is vulnerable to a man-in-the-middle (MiTM) attack, based on its acceptance of a specially crafted handshake.

This flaw could allow a MiTM attacker to decrypt or forge SSL messages by telling the service to begin encrypted communications before key material has been exchanged, which causes predictable keys to be used to secure future traffic.

Note ,only tested for an SSL/TLS MiTM vulnerability (CVE-2014-0224). However, we have inferred that the OpenSSL service on the remote host is also affected by six additional vulnerabilities that was disclosed in OpenSSL's June 5th, 2014 security advisory :

- An error exists in the 'ssl3_read_bytes' function that permits data to be injected into other sessions or allows denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2010-5298)

- An error exists related to the implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) that allows nonce disclosure via the 'FLUSH+RELOAD' cache side-channel attack. (CVE-2014-0076)

- A buffer overflow error exists related to invalid DTLS fragment handling that permits the execution of arbitrary code or allows denial of service attacks. Note that this issue only affects OpenSSL when used as a DTLS client or server. (CVE-2014-0195)

- An error exists in the 'do_ssl3_write' function that permits a NULL pointer to be dereferenced, which could allow denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2014-0198)

- An error exists related to DTLS handshake handling that could allow denial of service attacks. Note that this issue only affects OpenSSL when used as a DTLS client. (CVE-2014-0221)

- An error exists in the 'dtls1_get_message_fragment' function related to anonymous ECDH cipher suites. This could allow denial of service attacks. Note that this issue only affects OpenSSL TLS clients. (CVE-2014-3470)

OpenSSL did not release individual patches for these vulnerabilities, instead they were all patched under a single version release. Note that the service will remain vulnerable after patching until the service or host is restarted.

See also :
https://www.imperialviolet.org/2014/06/05/earlyccs.html
https://www.openssl.org/news/secadv_20140605.txt

Solution :
OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za. OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m. OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h.

Risk factor :
High / CVSS Base Score : 9.3
(CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)
CVSS Temporal Score : 8.1
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

High (9.0)		HP System Management Homepage ginkgosnmp.inc Command Injection

Synopsis :
The remote web server is affected by a command injection vulnerability.

Description:
According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server is earlier than 7.2.2 and is, therefore, reportedly affected by a command injection vulnerability.

An input validation error exists in the file 'ginkgosnmp.inc' related to the last segment in a requested URL path. This input is later used in an 'exec' call and could allow an authenticated attacker to execute arbitrary commands.

See also :
http://www.securityfocus.com/archive/1/528713/30/0/threaded

Solution :
Upgrade to HP System Management Homepage 7.2.2 or later.

Risk factor :
High / CVSS Base Score : 9.0
(CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)
CVSS Temporal Score : 7.4
(CVSS2#E:F/RL:OF/RC:C)
Public Exploit Available : true

High (7.8)		HP System Management Homepage < 7.2.1.0 Multiple Vulnerabilities

Synopsis :
The remote web server is affected by multiple vulnerabilities.

Description :
According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server is a version prior to 7.2.1.0 and is, therefore, reportedly affected by the following vulnerabilities :

- An error exists in the SSLv3 and TLSv1.0 specification that could allow the BEAST attack. (CVE-2011-3389)

- The utility 'apachectl' can receive a zero-length directory name in the LD_LIBRARY_PATH via the 'envvars' file. A local attacker with access to that utility could exploit this to load a malicious Dynamic Shared Object (DSO), leading to arbitrary code execution. (CVE-2012-0883)

- Numerous, unspecified errors could allow remote denial of service attacks. (CVE-2012-2110, CVE-2012-2329, CVE-2012-2336, CVE-2013-2357, CVE-2013-2358, CVE-2013-2359, CVE-2013-2360)

- The fix for CVE-2012-1823 does not completely correct the CGI query parameter vulnerability. Disclosure of PHP source code and code execution are still possible. Note that this vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration. (CVE-2012-2311, CVE-2012-2335)

- Unspecified errors exist that could allow unauthorized access. (CVE-2012-5217, CVE-2013-2355)

- Unspecified errors exist that could allow disclosure of sensitive information. (CVE-2013-2356, CVE-2013-2363)

- An unspecified error exists that could allow cross-site scripting attacks. (CVE-2013-2361)

- Unspecified errors exist that could allow a local attacker to cause denial of service conditions. (CVE-2013-2362, CVE-2013-2364)

- An as-yet unspecified vulnerability exists that could cause a denial of service condition. (CVE-2013-4821)

See also :
http://www.zerodayinitiative.com/advisories/ZDI-13-204/
http://www.securityfocus.com/archive/1/528723/30/0/threaded

Solution :
Upgrade to HP System Management Homepage 7.2.1.0 or later.

Risk factor :
High / CVSS Base Score : 7.8
(CVSS2#AV:N/AC:L/Au:N/C:C/I:N/A:N)
CVSS Temporal Score : 6.1
(CVSS2#E:POC/RL:OF/RC:C)
Public Exploit Available : true

High (7.5)		HP System Management Homepage < 7.4 Multiple Vulnerabilities

Synopsis :

The remote web server is affected by multiple vulnerabilities.

Description :

According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server is affected by the following vulnerabilities :

- A flaw exists within the included cURL that disables the 'CURLOPT_SSLVERIFYHOST' check when the setting on 'CURLOPT_SSL_VERIFYPEER' is disabled. This can allow a remote attacker to disable SSL certificate host name checks. (CVE-2013-4545)

- A flaw exists in the included PHP 'openssl_x509_parse' function due to user input not being properly sanitized. Using a specially crafted certificate, a remote attacker can exploit this to cause a denial of service or execute arbitrary code. (CVE-2013-6420)

- A flaw exists within the included cURL where the verification check for the CN and SAN name fields is skipped due to the digital signature verification being disabled. A remote attacker can exploit this to spoof servers or conduct a man-in-the-middle attack. (CVE-2013-6422)

- A flaw exists in the scan function within the included PHP 'ext/date/lib/parse_iso_intervals.c' script where user input is not properly sanitized. This can allow a remote attacker to cause a denial of service using a heap-based buffer overflow. (CVE-2013-6712)

- An unspecified cross-site scripting flaw exists which can allow a remote attacker, using a specially crafted request, to execute arbitrary code within the browser / server trust relationship. (CVE-2014-2640)

- An unspecified cross-site request forgery vulnerability exists. (CVE-2014-2641)

- An unspecified vulnerability exists that can allow a remote attacker to conduct clickjacking attacks. (CVE-2014-2642)

See also :

http://www.securityfocus.com/archive/1/533589/30/0/threaded

Solution :

Upgrade to HP System Management Homepage 7.4 or later.

Risk factor :

High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 6.5
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : false

Medium (6.8)		HP System Management Homepage < 7.3 Multiple Vulnerabilities

Synopsis :
The remote web server is affected by multiple vulnerabilities.

Description :
According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server may be affected by the following vulnerabilities :

- Versions prior to 7.3 are affected by an unspecified information disclosure vulnerability. (CVE-2013-4846)

- Versions 7.1 through 7.2.2 are affected by an unspecified cross-site request forgery vulnerability. (CVE-2013-6188)

See also :
http://www.securityfocus.com/archive/1/531406/30/0/threaded

Solution :
Upgrade to HP System Management Homepage 7.3 or later.

Risk factor :
Medium / CVSS Base Score : 6.8
(CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 5.9
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

Medium (6.4)		SSL Certificate Cannot Be Trusted

Synopsis :
The SSL certificate for this service cannot be trusted.

Description :
The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

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 unrecognised, 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 is not recognised.
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.

Solution :
Purchase or generate a proper certificate for this service.

Risk factor :
Medium / CVSS Base Score : 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Medium (6.4)		SSL Self-Signed Certificate

Synopsis :
The SSL certificate chain for this service ends in an unrecognised

self-signed certificate.

Description :
The X.509 certificate chain for this service is not signed by a recognised 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 unrecognised certificate authority.

Solution :
Purchase or generate a proper certificate for this service.

Risk factor :
Medium / CVSS Base Score : 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Medium (5.1)		Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle

Synopsis :
It may be possible to get access to the remote host.

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.

See also :
http://www.oxid.it/downloads/rdp-gbu.pdf
http://technet.microsoft.com/en-us/library/cc782610.aspx

Solution :
- 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.

Risk factor :
Medium / CVSS Base Score : 5.1
(CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 4.6
(CVSS2#E:F/RL:W/RC:ND)
Public Exploit Available : true

Medium (5.0)		SSL Certificate Expiry

Synopsis :
The remote server's SSL certificate has already expired.

Description :
This script checks expiry dates of certificates associated with SSL-enabled services on the target and reports whether any have already expired.

Solution :
Purchase or generate a new SSL certificate to replace the existing one.

Risk factor :
Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Medium (5.0)		SSL Version 2 and 3 Protocol Detection

Synopsis :
The remote service encrypts traffic using a protocol with known weaknesses.

Description :
The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0, which reportedly suffer from several cryptographic flaws. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

NIST has determined SSL v3.0 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.

See also :
http://www.schneier.com/paper-ssl.pdf
http://support.microsoft.com/kb/187498
http://www.linux4beginners.info/node/disable-sslv2
https://www.openssl.org/~bodo/ssl-poodle.pdf

Solution :
Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.0 or higher instead.

Risk factor :
Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Medium (5.0)		SSL Certificate with Wrong Hostname

Synopsis :
The SSL certificate for this service is for a different host.

Description :
The commonName (CN) of the SSL certificate presented on this service is for a different machine.

Solution :
Purchase or generate a proper certificate for this service.

Risk factor :
Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Medium (5.0)		SMB Signing Required

Synopsis :
Signing is not required on the remote SMB server.

Description :
Signing is not required on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.

See also :
http://support.microsoft.com/kb/887429
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

Solution :
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.

Risk factor :
Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS Temporal Score : 3.7
(CVSS2#E:U/RL:OF/RC:C)
Public Exploit Available : false

Medium (4.3)		Terminal Services Encryption Level is Medium or Low

Synopsis :
The remote host is using weak cryptography.

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.

Solution :
Change RDP encryption level to one of :

3. High

4. FIPS Compliant

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Medium (4.3)		Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Synopsis :
The remote Terminal Services doesn't use Network Level Authentication only.

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.

See also :
http://technet.microsoft.com/en-us/library/cc732713.aspx

Solution :
Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.
Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Medium (4.3)		SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability

Synopsis :
It may be possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description :
A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow
information disclosure if an attacker intercepts encrypted traffic
served from an affected system.

TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are
not affected.

This script tries to establish an SSL/TLS remote connection using an
affected SSL version and cipher suite, and then solicits return data.
If returned application data is not fragmented with an empty or
one-byte record, it is likely vulnerable.

OpenSSL uses empty fragments as a countermeasure unless the
'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when
OpenSSL
is initialized.

Microsoft implemented one-byte fragments as a countermeasure, and the
setting can be controlled via the registry key
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders
\SCHANNEL\SendExtraRecord.

Therefore, if multiple applications use the same SSL/TLS
implementation, some may be vulnerable while others may not, depending
on whether or not a countermeasure has been enabled.

Note that this script detects the vulnerability in the SSLv3/TLSv1
protocol implemented in the server. It does not detect the BEAST
attack where it exploits the vulnerability at HTTPS client-side
(i.e., Internet browser). The detection at server-side does not
necessarily mean your server is vulnerable to the BEAST attack
because the attack exploits the vulnerability at client-side, and
both SSL/TLS clients and servers can independently employ the split record
countermeasure.

See also :
http://www.openssl.org/~bodo/tls-cbc.txt
http://vnhacker.blogspot.com/2011/09/beast.html
http://technet.microsoft.com/en-us/security/bulletin/ms12-006
http://support.microsoft.com/kb/2643584
http://blogs.msdn.com/b/kaushal/archive/2012/01/21/fixing-the-beast.aspx

Solution :

Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported. Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available.

Note that additional configuration may be required after the installation of the MS12-006 security update in order to enable the split-record countermeasure. See Microsoft KB2643584 for details.

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 3.7
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

Medium (4.3)		SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis :
It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

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.

See also :
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

Solution :
Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 3.7
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

Low (2.6)		Terminal Services Encryption Level is not FI

Synopsis :
The remote host is not FIPS-140 compliant.

Description :
The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.

Solution :
Change RDP encryption level to :

4. FIPS Compliant

Risk factor :

Low / CVSS Base Score : 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Low (2.6)		SSL Anonymous Cipher Suites Supported

Synopsis :
The remote service supports the use of anonymous SSL ciphers.

Description :
The remote host supports the use of anonymous SSL ciphers. While this
enables an administrator to set up a service that encrypts traffic
without having to generate and configure SSL certificates, it offers
no way to verify the remote host's identity and renders the service
vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the
same physical network.

See also :
http://www.openssl.org/docs/apps/ciphers.html

Solution :
Reconfigure the affected application if possible to avoid use of weak
ciphers.

Risk factor :
Low / CVSS Base Score : 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 2.3
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

Low (2.6)		SSL RC4 Cipher Suites Supported

Synopsis :
The remote service supports the use of the RC4 cipher.

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.

See also :
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/

Solution :
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.

Risk factor :
Low / CVSS Base Score : 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 2.3
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : false

192.168.0.4

Summary

Critical	High	Medium	Low
0	0	7	4

Medium (6.4)		SSL Certificate Cannot Be Trusted

Synopsis :
The SSL certificate for this service cannot be trusted.

Description :
The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

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 unrecognised, 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 is not recognise.

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.

Solution :
Purchase or generate a proper certificate for this service.

Risk factor :
Medium

CVSS Base Score : 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Medium (6.4)		SSL Self-Signed Certificate

Synopsis :
The SSL certificate chain for this service ends in an unrecognised self-signed certificate.

Description :
The X.509 certificate chain for this service is not signed by a recognised 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 unrecognised certificate authority.

Solution :
Purchase or generate a proper certificate for this service.

Risk factor :
Medium

CVSS Base Score : 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Medium (5.0)		SSL Certificate Expiry

Synopsis :
The remote server's SSL certificate has already expired.

Description :
This script checks expiry dates of certificates associated with SSL-enabled services on the target and reports whether any have already expired.

Solution :
Purchase or generate a new SSL certificate to replace the existing one.

Risk factor :
Medium

CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Medium (5.0)		SSL Version 2 and 3 Protocol Detection

Synopsis :
The remote service encrypts traffic using a protocol with known weaknesses.

Description :
The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0, which reportedly suffer from several cryptographic flaws. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

NIST has determined SSL v3.0 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.

See also :
http://www.schneier.com/paper-ssl.pdf
http://support.microsoft.com/kb/187498
http://www.linux4beginners.info/node/disable-sslv2
https://www.openssl.org/~bodo/ssl-poodle.pdf

Solution :
Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.0 or higher instead.

Risk factor :
Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Medium (4.3)		HTTP TRACE / TRACK Methods Allowed

Synopsis :
Debugging functions are enabled on the remote web server.

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.

See also :
http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
http://download.oracle.com/sunalerts/1000718.1.html

Solution :
Disable these methods. Refer to the plugin output for more information.

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 3.9

(CVSS2#E:F/RL:W/RC:C)
Public Exploit Available : true

Medium (4.3)		SSL Medium Strength Cipher Suites Supported

Synopsis :
The remote service supports the use of medium strength SSL ciphers.

Description :
The remote host supports the use of SSL ciphers that offer medium strength encryption, which we currently regard as those with key lengths at least 56 bits and less than 112 bits.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

Solution :
Reconfigure the affected application if possible to avoid use of medium strength ciphers.
Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Medium (4.3)	58751	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability

Synopsis :
It may be possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description :
A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted traffic served from an affected system.

TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected.

This script tries to establish an SSL/TLS remote connection using an affected SSL version and cipher suite, and then solicits return data. If returned application data is not fragmented with an empty or one-byte record, it is likely vulnerable.

OpenSSL uses empty fragments as a countermeasure unless the

'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when OpenSSL
is initialized.

Microsoft implemented one-byte fragments as a countermeasure, and the setting can be controlled via the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\SendExtraRecord.

Therefore, if multiple applications use the same SSL/TLS implementation, some may be vulnerable while others may not, depending on whether or not a countermeasure has been enabled.

Note that this script detects the vulnerability in the SSLv3/TLSv1 protocol implemented in the server. It does not detect the BEAST attack where it exploits the vulnerability at HTTPS client-side (i.e., Internet browser). The detection at server-side does not necessarily mean your server is vulnerable to the BEAST attack because the attack exploits the vulnerability at client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure.

See also :
http://www.openssl.org/~bodo/tls-cbc.txt
http://vnhacker.blogspot.com/2011/09/beast.html
http://technet.microsoft.com/en-us/security/bulletin/ms12-006
http://support.microsoft.com/kb/2643584
http://blogs.msdn.com/b/kaushal/archive/2012/01/21/fixing-the-beast.aspx

Solution :
Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported. Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available.

Note that additional configuration may be required after the installation of the MS12-006 security update in order to enable the split-record countermeasure. See Microsoft KB2643584 for details.

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 3.7
(CVSS2#E:ND/RL:OF/RC:C)

Public Exploit Available : true

Low (2.6)	SSL RC4 Cipher Suites Supported

Synopsis :
The remote service supports the use of the RC4 cipher.

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.

See also :
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/

Solution :
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.

Risk factor :
Low / CVSS Base Score : 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 2.3
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : false

Low (2.6)	SSH Server CBC Mode Ciphers Enabled

Synopsis :
The SSH server is configured to use Cipher Block Chaining.

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.

Solution :
Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk factor :
Low / CVSS Base Score : 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 2.3
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : false

Low (2.6)		SSH Weak MAC Algorithms Enabled

Synopsis :
SSH is configured to allow MD5 and 96-bit MAC algorithms.

Description :
The 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 does not check for vulnerable software versions.

Solution :
Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk factor :
Low / CVSS Base Score : 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
Public Exploit Available : false

Low		SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis :
The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Description :
At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.

Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

See also :
https://www.cabforum.org/Baseline_Requirements_V1.pdf

Solution :
Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Risk factor :
Low

192.168.0.35

Summary

Critical	High	Medium	Low
0	1	6	2

High (7.5)	Oracle TNS Listener Remote Poisoning

Synopsis :
It is possible to register with a remote Oracle TNS listener.

Description :
The remote Oracle TNS listener allows service registration from a remote host. An attacker can exploit this issue to divert data from a legitimate database server or client to an attacker-specified system.

Successful exploits will allow the attacker to manipulate database instances, potentially facilitating man-in-the-middle, session-hijacking, or denial of service attacks on a legitimate database server.

Solution :
Apply the work-around in Oracle's advisory.

Risk factor :
High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 6.5
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

Medium (6.4)	SSL Certificate Cannot Be Trusted

Synopsis :
The SSL certificate for this service cannot be trusted.

Description :
The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

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 unrecognised, 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 is not recognise.

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.

Solution :
Purchase or generate a proper certificate for this service.

Risk factor :
Medium / CVSS Base Score : 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Medium (6.4)		SSL Self-Signed Certificate

Synopsis :
The SSL certificate chain for this service ends in an unrecognised self-signed certificate.

Description :

The X.509 certificate chain for this service is not signed by a recognised 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 unrecognised certificate authority.

Solution :
Purchase or generate a proper certificate for this service.

Risk factor :
Medium / CVSS Base Score : 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Medium (5.1)		Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle

Synopsis :
It may be possible to get access to the remote host.

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.

See also :
http://www.oxid.it/downloads/rdp-gbu.pdf
http://technet.microsoft.com/en-us/library/cc782610.aspx

Solution :
- 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.

Risk factor :
Medium / CVSS Base Score : 5.1
(CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 4.6
(CVSS2#E:F/RL:W/RC:ND)
Public Exploit Available : true

Medium (5.0)		SMB Signing Required

Synopsis :
Signing is not required on the remote SMB server.

Description :
Signing is not required on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.

See also :
http://support.microsoft.com/kb/887429
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

Solution :
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.

Risk factor :
Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS Temporal Score : 3.7
(CVSS2#E:U/RL:OF/RC:C)
Public Exploit Available : false

Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low

Synopsis :
The remote host is using weak cryptography.

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.

Solution :
Change RDP encryption level to one of :

3. High

4. FIPS Compliant

Risk factor :

Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Medium (4.3)		Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Synopsis :
The remote Terminal Services doesn't use Network Level Authentication only.

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.

See also :
http://technet.microsoft.com/en-us/library/cc732713.aspx

Solution :
Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Low (2.6)		Terminal Services Encryption Level is not FIPS-140 Compliant

Synopsis :
The remote host is not FIPS-140 compliant.

Description :
The encryption setting used by the remote Terminal Services service
is not FIPS-140 compliant.

Solution :
Change RDP encryption level to :
4. FIPS Compliant

Risk factor :
Low / CVSS Base Score : 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Low (2.6)		SSL RC4 Cipher Suites Supported

Synopsis :
The remote service supports the use of the RC4 cipher.

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.
See also:
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/

Solution:
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.

Risk factor:
Low / CVSS Base Score: 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 2.3
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : false

192.168.0.44

Summary

Critical	High	Medium	Low
0	0	1	0

Medium (5.0)		SMB Signing Required

Synopsis :
Signing is not required on the remote SMB server.

Description :
Signing is not required on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.

See also :
http://support.microsoft.com/kb/887429
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

Solution :
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.

Risk factor :
Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS Temporal Score : 3.7
(CVSS2#E:U/RL:OF/RC:C)
Public Exploit Available : false

192.168.0.47

Summary

Critical	High	Medium	Low
0	1	0	0

High (7.5)		TCP/IP Initial Sequence Number (ISN) Reuse Weakness

Synopsis :
The remote device seems to generate predictable TCP Initial Sequence Numbers.

Description :
The remote host seems to generate Initial Sequence Numbers (ISN) in a weak manner which seems to solely depend on the source and dest port of the TCP packets.

An attacker may exploit this flaw to establish spoofed connections to the remote host.

The Raptor Firewall and Novell NetWare are known to be vulnerable to this flaw, although other network devices may be vulnerable as well.

See also :
http://archives.neohapsis.com/archives/bugtraq/2002-07/0492.html
http://securityresponse.symantec.com/avcenter/security/Content/2002.08.05.html

Solution :
If you are using a Raptor Firewall, install the TCP security hotfix described in Symantec's advisory. Otherwise, contact your vendor for a patch.

Risk factor :
High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 5.5
(CVSS2#E:U/RL:OF/RC:C)
Public Exploit Available : false

192.168.0.87

Summary

Critical	High	Medium	Low
0	0	1	2

Medium (5.8)		Unencrypted Telnet Server

Synopsis :
The remote Telnet server transmits traffic in cleartext.

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.

Solution :
Disable the Telnet service and use SSH instead.

Risk factor :
Medium / CVSS Base Score : 5.8
(CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Low (3.3)		Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)

Synopsis :
The remote host appears to leak memory in network packets.

Description :
The remote host uses a network device driver that pads ethernet frames with data which vary from one packet to another, likely taken from kernel memory, system memory allocated to the device driver, or a

hardware buffer on its network interface card.

Known as 'Etherleak', this information disclosure vulnerability may allow an attacker to collect sensitive information from the affected host provided he is on the same physical subnet as that host.
Solution :
Contact the network device driver's vendor for a fix.

Risk factor :
Low / CVSS Base Score : 3.3
(CVSS2#AV:A/AC:L/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 2.9
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : false

Low (3.2)		IP Forwarding Enabled

Synopsis :
The remote host has IP forwarding enabled.

Description :
The remote host has IP forwarding enabled. An attacker may use this flaw to route packets through this host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution :
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\Parameter
```

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.

Risk factor :
Low / CVSS Base Score : 3.2

(CVSS2#AV:A/AC:H/Au:N/C:P/I:P/A:N)

192.168.0.251

Summary

Critical	High	Medium	Low
0	1	5	2

High (7.5)		SNMP Agent Default Community Name

Synopsis :
The community name of the remote SNMP server can be guessed.

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).

Solution :
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.

Risk factor :
High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 7.1
(CVSS2#E:F/RL:U/RC:ND)

Medium (6.4)		SSL Certificate Cannot Be Trusted

Synopsis :
The SSL certificate for this service cannot be trusted.

Description :
The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

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 unrecognised, 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 is not recognise.

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.

Solution :
Purchase or generate a proper certificate for this service.

Risk factor :
Medium / CVSS Base Score : 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Medium (6.4)		SSL Self-Signed Certificate

Synopsis :
The SSL certificate chain for this service ends in an unrecognised
self-signed certificate.

Description :
The X.509 certificate chain for this service is not signed by a
recognised 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
unrecognised certificate authority.

Solution :

Purchase or generate a proper certificate for this service.
Risk factor :
Medium / CVSS Base Score : 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Medium (5.0)		SSL Version 2 and 3 Protocol Detection

Synopsis :
The remote service encrypts traffic using a protocol with known weaknesses.

Description :
The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0, which reportedly suffer from several cryptographic flaws. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.

NIST has determined SSL v3.0 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.

See also :
http://www.schneier.com/paper-ssl.pdf
http://support.microsoft.com/kb/187498
http://www.linux4beginners.info/node/disable-sslv2
https://www.openssl.org/~bodo/ssl-poodle.pdf

Solution :
Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.0 or higher instead.

Risk factor :
Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Medium (4.3)		SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis :
It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

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.

See also :
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

Solution :
Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 3.7

(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

Medium (4.0)		SSL Certificate Signed using Weak Hashing Algorithm

Synopsis :
An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description :
The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm - MD2, MD4, or MD5. These signature algorithms are known to be vulnerable to collision attacks. In theory, a determined attacker may be able to leverage this weakness to generate another certificate with the same digital signature, which could allow the attacker to masquerade as the affected service.

See also :
http://tools.ietf.org/html/rfc3279
http://www.phreedom.org/research/rogue-ca/
http://technet.microsoft.com/en-us/security/advisory/961509

Solution :
Contact the Certificate Authority to have the certificate reissued.

Risk factor :
Medium / CVSS Base Score : 4.0
(CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N)
CVSS Temporal Score : 3.5
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

Low (2.6)		SSL RC4 Cipher Suites Supported

Synopsis :
The remote service supports the use of the RC4 cipher.

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.
See also :
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/

Solution :
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.

Risk factor :
Low / CVSS Base Score : 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 2.3
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : false

Low		SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis :
The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Description :
At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.

Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

See also :
https://www.cabforum.org/Baseline_Requirements_V1.pdf

Solution :
Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Risk factor :
Low

192.168.0.252

Summary

Critical	High	Medium	Low
0	5	12	5

High (9.3)		HP System Management Homepage < 7.2.0.14 iprange Parameter Code Execution

Synopsis :
The remote web server is affected by a code execution vulnerability.

Description :
According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server is a version prior to 7.2.0.14 and is, therefore, reportedly affected by a code execution vulnerability related to the 'iprange' parameter in requests made to '/proxy/DataValidation'

Note that successful exploitation requires that anonymous access is enabled.

Solution :

Upgrade to HP System Management Homepage 7.2.0.14 or later.

Risk factor :
High / CVSS Base Score : 9.3
(CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)
CVSS Temporal Score : 7.7
(CVSS2#E:F/RL:OF/RC:ND)
Public Exploit Available : true

High (9.3)		HP System Management Homepage < 7.2.4.1 / 7.3.3.1 OpenSSL Multiple Vulnerabilities

Synopsis :
The remote web server is affected by multiple vulnerabilities.

Description :
According to the web server's banner, the version of HP System

Management Homepage (SMH) hosted on the remote web server has an
implementation of the OpenSSL library affected by the following
vulnerabilities :

- An error exists in the function 'ssl3_read_bytes'
that could allow data to be injected into other
sessions or allow denial of service attacks. Note
this issue is only exploitable if
'SSL_MODE_RELEASE_BUFFERS' is enabled. (CVE-2010-5298)

- An error exists related to the implementation of the
Elliptic Curve Digital Signature Algorithm (ECDSA) that
could allow nonce disclosure via the 'FLUSH+RELOAD'
cache side-channel attack. (CVE-2014-0076)

- A buffer overflow error exists related to invalid DTLS
fragment handling that could lead to execution of
arbitrary code. Note this issue only affects OpenSSL
when used as a DTLS client or server. (CVE-2014-0195)

- An error exists in the function 'do_ssl3_write' that
could allow a NULL pointer to be dereferenced leading
to denial of service attacks. Note this issue is
exploitable only if 'SSL_MODE_RELEASE_BUFFERS' is
enabled. (CVE-2014-0198)

- An error exists related to DTLS handshake handling that
could lead to denial of service attacks. Note this
issue only affects OpenSSL when used as a DTLS client.
(CVE-2014-0221)

- An unspecified error exists that could allow an
attacker to cause usage of weak keying material
leading to simplified man-in-the-middle attacks.
(CVE-2014-0224)

- An unspecified error exists related to anonymous ECDH
ciphersuites that could allow denial of service
attacks. Note this issue only affects OpenSSL TLS
clients. (CVE-2014-3470)

See also :
http://www.securityfocus.com/archive/1/532538/30/0/threaded
http://www.securityfocus.com/archive/1/532642/30/0/threaded

http://www.openssl.org/news/vulnerabilities.html#CVE-2010-5298
http://www.openssl.org/news/vulnerabilities.html#2014-0076
http://www.openssl.org/news/vulnerabilities.html#CVE-2014-0198
http://www.openssl.org/news/vulnerabilities.html#CVE-2014-0221
http://www.openssl.org/news/vulnerabilities.html#CVE-2014-0224
http://www.openssl.org/news/vulnerabilities.html#CVE-2014-3470
http://www.openssl.org/news/secadv_20140605.txt

Solution :
Upgrade to HP System Management Homepage 7.2.4.1 (Windows 2003) / 7.3.3.1 (Linux or Windows) or later.

Note that version 7.3.3.1 for Linux x86 still contains OpenSSL v1.0.0d.

Ensure that any products with which such an install might communiate have been updated to the latest versions to not be affected by the vulnerability covered by CVE-2014-0224.

Risk factor :
High / CVSS Base Score : 9.3
(CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)
CVSS Temporal Score : 8.1
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

High (9.0)		HP System Management Homepage ginkgosnmp.inc Command Injection

Synopsis :
The remote web server is affected by a command injection vulnerability.

Description :
According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server is earlier than 7.2.2 and is, therefore, reportedly affected by a command injection vulnerability.

An input validation error exists in the file 'ginkgosnmp.inc' related to the last segment in a requested URL path. This input is later used in an 'exec' call and could allow an authenticated attacker to execute arbitrary commands.

See also :
http://www.securityfocus.com/archive/1/528713/30/0/threaded

Solution :
Upgrade to HP System Management Homepage 7.2.2 or later.

Risk factor :
High / CVSS Base Score : 9.0
(CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)
CVSS Temporal Score : 7.4
(CVSS2#E:F/RL:OF/RC:C)
Public Exploit Available : true

High (7.8)		HP System Management Homepage < 7.2.1.0 Multiple Vulnerabilities

Synopsis :
The remote web server is affected by multiple vulnerabilities.

Description :
According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server is a version prior to 7.2.1.0 and is, therefore, reportedly affected by the following vulnerabilities :

- An error exists in the SSLv3 and TLSv1.0 specification that could allow the BEAST attack. (CVE-2011-3389)

- The utility 'apachectl' can receive a zero-length directory name in the LD_LIBRARY_PATH via the 'envvars' file. A local attacker with access to that utility could exploit this to load a malicious Dynamic Shared Object (DSO), leading to arbitrary code execution. (CVE-2012-0883)

- Numerous, unspecified errors could allow remote denial of service attacks. (CVE-2012-2110, CVE-2012-2329, CVE-2012-2336, CVE-2013-2357, CVE-2013-2358, CVE-2013-2359, CVE-2013-2360)

- The fix for CVE-2012-1823 does not completely correct the CGI query parameter vulnerability. Disclosure of PHP source code and code execution are still possible. Note that this vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod_php' is not an exploitable configuration.

(CVE-2012-2311, CVE-2012-2335)

- Unspecified errors exist that could allow unauthorized access. (CVE-2012-5217, CVE-2013-2355)

- Unspecified errors exist that could allow disclosure of sensitive information. (CVE-2013-2356, CVE-2013-2363)

- An unspecified error exists that could allow cross-site scripting attacks. (CVE-2013-2361)

- Unspecified errors exist that could allow a local attacker to cause denial of service conditions. (CVE-2013-2362, CVE-2013-2364)

- An as-yet unspecified vulnerability exists that could cause a denial of service condition. (CVE-2013-4821)

See also :
http://www.zerodayinitiative.com/advisories/ZDI-13-204/
http://www.securityfocus.com/archive/1/528723/30/0/threaded

Solution :
Upgrade to HP System Management Homepage 7.2.1.0 or later.

Risk factor :
High / CVSS Base Score : 7.8
(CVSS2#AV:N/AC:L/Au:N/C:C/I:N/A:N)
CVSS Temporal Score : 6.1
(CVSS2#E:POC/RL:OF/RC:C)
Public Exploit Available : true

High (7.5)		HP System Management Homepage < 7.4 Multiple Vulnerabilities

Synopsis :
The remote web server is affected by multiple vulnerabilities.

Description :
According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server is affected by the following vulnerabilities :

- A flaw exists within the included cURL that disables the

'CURLOPT_SSLVERIFYHOST' check when the setting on 'CURLOPT_SSL_VERIFYPEER' is disabled. This can allow a remote attacker to disable SSL certificate host name checks. (CVE-2013-4545)

- A flaw exists in the included PHP 'openssl_x509_parse' function due to user input not being properly sanitized. Using a specially crafted certificate, a remote attacker can exploit this to cause a denial of service or execute arbitrary code. (CVE-2013-6420)

- A flaw exists within the included cURL where the verification check for the CN and SAN name fields is skipped due to the digital signature verification being disabled. A remote attacker can exploit this to spoof servers or conduct a man-in-the-middle attack. (CVE-2013-6422)

- A flaw exists in the scan function within the included PHP 'ext/date/lib/parse_iso_intervals.c' script where user input is not properly sanitized. This can allow a remote attacker to cause a denial of service using a heap-based buffer overflow. (CVE-2013-6712)

- An unspecified cross-site scripting flaw exists which can allow a remote attacker, using a specially crafted request, to execute arbitrary code within the browser / server trust relationship. (CVE-2014-2640)

- An unspecified cross-site request forgery vulnerability exists. (CVE-2014-2641)

- An unspecified vulnerability exists that can allow a remote attacker to conduct clickjacking attacks. (CVE-2014-2642)

See also :
http://www.securityfocus.com/archive/1/533589/30/0/threaded

Solution :
Upgrade to HP System Management Homepage 7.4 or later.

Risk factor :
High / CVSS Base Score : 7.5

(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 6.5
(CVSS2#E:ND/RL:OF/RC:C)

Medium (6.8)		HP System Management Homepage < 7.3 Multiple Vulnerabilities

Synopsis :
The remote web server is affected by multiple vulnerabilities.

Description :
According to the web server's banner, the version of HP System Management Homepage (SMH) hosted on the remote web server may be affected by the following vulnerabilities :

- Versions prior to 7.3 are affected by an unspecified information disclosure vulnerability. (CVE-2013-4846)

- Versions 7.1 through 7.2.2 are affected by an unspecified cross-site request forgery vulnerability. (CVE-2013-6188)

See also :
http://www.securityfocus.com/archive/1/531406/30/0/threaded

Solution :
Upgrade to HP System Management Homepage 7.3 or later.

Risk factor :
Medium / CVSS Base Score : 6.8
(CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 5.9
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

Medium (6.4)		SSL Certificate Cannot Be Trusted

Synopsis :
The SSL certificate for this service cannot be trusted.

Description :
The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

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 unrecognised, 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 is not recognise.

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.

Solution :
Purchase or generate a proper certificate for this service.

Risk factor :
Medium / CVSS Base Score : 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Medium (6.4)		SSL Self-Signed Certificate

Synopsis :
The SSL certificate chain for this service ends in an unrecognised self-signed certificate.

Description :
The X.509 certificate chain for this service is not signed by a recognised 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 unrecognised certificate authority.

Solution :
Purchase or generate a proper certificate for this service.

Risk factor :
Medium / CVSS Base Score : 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Medium (5.8)		SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

Synopsis :
The remote service allows insecure renegotiation of TLS / SSL connections.

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.

See also :
http://www.ietf.org/mail-archive/web/tls/current/msg03948.html
http://www.g-sec.lu/practicaltls.pdf
http://tools.ietf.org/html/rfc5746

Solution :
Contact the vendor for specific patch information.

Risk factor :
Medium / CVSS Base Score : 5.8
(CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:P)
CVSS Temporal Score : 5.0
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

Medium (5.1)		Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle

Synopsis :
It may be possible to get access to the remote host.

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.

See also :
http://www.oxid.it/downloads/rdp-gbu.pdf
http://technet.microsoft.com/en-us/library/cc782610.aspx

Solution :
- 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.

Risk factor :
Medium / CVSS Base Score : 5.1
(CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 4.6
(CVSS2#E:F/RL:W/RC:ND)
Public Exploit Available : true

Medium (5.0)		SSL Version 2 and 3 Protocol Detection

Synopsis :
The remote service encrypts traffic using a protocol with known
weaknesses.

Description :
The remote service accepts connections encrypted using SSL 2.0 and/or
SSL 3.0, which reportedly suffer from several cryptographic flaws. An
attacker may be able to exploit these issues to conduct
man-in-the-middle attacks or decrypt communications between the
affected service and clients.

NIST has determined SSL v3.0 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.

See also :
http://www.schneier.com/paper-ssl.pdf
http://support.microsoft.com/kb/187498
http://www.linux4beginners.info/node/disable-sslv2
https://www.openssl.org/~bodo/ssl-poodle.pdf

Solution :
Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.0 or higher instead.

Risk factor :
Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Medium (5.0)		SMB Signing Required

Synopsis :
Signing is not required on the remote SMB server.

Description :
Signing is not required on the remote SMB server. This can allow
man-in-the-middle attacks against the SMB server.

See also :

http://support.microsoft.com/kb/887429
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html
Solution:
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.

Risk factor :
Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)
CVSS Temporal Score : 3.7
(CVSS2#E:U/RL:OF/RC:C)
Public Exploit Available : false

Medium (4.3)		SSL Weak Cipher Suites Supported

Synopsis :
The remote service supports the use of weak SSL ciphers.

Description :
The remote host supports the use of SSL ciphers that offer weak encryption.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See also :
http://www.openssl.org/docs/apps/ciphers.html

Solution :
Reconfigure the affected application, if possible to avoid the use of weak ciphers.

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Medium (4.3)		Terminal Services Encryption Level is Medium or Low

Synopsis :
The remote host is using weak cryptography.

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.

Solution :
Change RDP encryption level to one of :

3. High

4. FIPS Compliant

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Medium (4.3)		Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Synopsis :
The remote Terminal Services doesn't use Network Level Authentication only.

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.

See also :
http://technet.microsoft.com/en-us/library/cc732713.aspx

Solution :
Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Medium (4.3)		SSL/TLS Protocol Initialization Vector Implementation Information Disclosure

Synopsis :
It may be possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description :
A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted traffic served from an affected system.

TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected.

This script tries to establish an SSL/TLS remote connection using an affected SSL version and cipher suite, and then solicits return data. If returned application data is not fragmented with an empty or one-byte record, it is likely vulnerable.

OpenSSL uses empty fragments as a countermeasure unless the 'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when OpenSSL is initialized.

Microsoft implemented one-byte fragments as a countermeasure, and the setting can be controlled via the registry key
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders
\SCHANNEL\SendExtraRecord.

Therefore, if multiple applications use the same SSL/TLS implementation, some may be vulnerable while others may not, depending on whether or not a countermeasure has been enabled.

Note that this script detects the vulnerability in the SSLv3/TLSv1 protocol implemented in the server. It does not detect the BEAST attack where it exploits the vulnerability at HTTPS client-side (i.e., Internet browser). The detection at server-side does not necessarily mean your server is vulnerable to the BEAST attack because the attack exploits the vulnerability at client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure.

See also :
http://www.openssl.org/~bodo/tls-cbc.txt
http://vnhacker.blogspot.com/2011/09/beast.html
http://technet.microsoft.com/en-us/security/bulletin/ms12-006
http://support.microsoft.com/kb/2643584
http://blogs.msdn.com/b/kaushal/archive/2012/01/21/fixing-the-beast.aspx

Solution :
Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported. Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available.

Note that additional configuration may be required after the installation of the MS12-006 security update in order to enable the split-record countermeasure. See Microsoft KB2643584 for details.

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 3.7
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

Medium (4.3)		SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis :
It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

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.

See also :
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

Solution :
Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk factor :
Medium / CVSS Base Score : 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 3.7
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

Low (3.2)		IP Forwarding Enabled

Synopsis :
The remote host has IP forwarding enabled.

Description :
The remote host has IP forwarding enabled. An attacker may use this flaw to route packets through this host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution :
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\Parameter
```

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.

Risk factor :
Low / CVSS Base Score : 3.2
(CVSS2#AV:A/AC:H/Au:N/C:P/I:P/A:N)

Low (2.6)		Terminal Services Encryption Level is not FIPS-140 Compliant

Synopsis :
The remote host is not FIPS-140 compliant.

Description :
The encryption setting used by the remote Terminal Services service
is not FIPS-140 compliant.

Solution :
Change RDP encryption level to :

4. FIPS Compliant

Risk factor :
Low / CVSS Base Score : 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Low (2.6)		SSL Anonymous Cipher Suites Supported

Synopsis :
The remote service supports the use of anonymous SSL ciphers.

Description :
The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See also :
http://www.openssl.org/docs/apps/ciphers.html

Solution :
Reconfigure the affected application if possible to avoid use of weak ciphers.

Risk factor :
Low / CVSS Base Score : 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 2.3
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : true

Low (2.6)		SSL RC4 Cipher Suites Supported

Synopsis :
The remote service supports the use of the RC4 cipher.

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.

See also :
http://cr.yp.to/talks/2013.03.12/slides.pdf
Solution :

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.

Risk factor :
Low / CVSS Base Score : 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)
CVSS Temporal Score : 2.3
(CVSS2#E:ND/RL:OF/RC:C)
Public Exploit Available : false

Low		SSL Certificate Chain Contains RSA Keys L

Synopsis :
The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Description :
At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.

Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

See also :
https://www.cabforum.org/Baseline_Requirements_V1.pdf

Solution :
Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Risk factor :
Low

192.168.0.253

Summary

Critical	High	Medium	Low

0	1	0	0

High (7.5)		SNMP Agent Default Community Name

Synopsis :
The community name of the remote SNMP server can be guessed.

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).

Solution :
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.

Risk factor :
High / CVSS Base Score : 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS Temporal Score : 7.1
(CVSS2#E:F/RL:U/RC:ND)

Conclusion and Recommendations

As you can see there are a lot of security issues in your network, some very minor and some that need attention right away. For most of the issues noted there are easy fixes for those that do not have a patch or a recommended fix some creative filtering and locking down of the system in general should help remedy the problem.

I would also recommend a more robust monitoring of the internal network and its activities in order to spot suspicions activity and trace them. This could also be integrated with regular penetration tests to ensure no new vulnerabilities have been created from configuration changes or updates to your systems.

I did not spot any signs that your system had already been compromised however some of the vulnerabilities found have been open to exploit for some time for example, Heartbleed vulnerability publicly announced April 7 2014 meaning this particular security issue has been on your system just under one year. Some other vulnerabilities are likely to have been there longer. If you are worried that you may have been compromised the recommended action to take would be to wipe, rebuild and reinstall all systems on the network allowing the disks to be wiped will remove any unwanted backdoors.

I would also recommend a follow up test to ensure no further issues have been created in the patching of the vulnerabilities, this we will provide free of charge for you.
I would also recommend and external penetration test to establish what vulnerabilities may lead in from outside your network.

To recap the recommendations:

Re-test (After fixes have been applied)
Increased Monitoring Solution.
Regular penetration tests, automated or manual.
External penetration test.

We can supply you with all these services and more to fit your needs at very good prices with many offers, we can also do an introductory trial rate and offer many free trials.