Nessus Report

Nessus Scan Report

Mon, 19 Dec 2016 15:57:29 SGT

Table Of Contents

Vulnerabilities By Host

192.168.108.15

Scan Information

Start time:	Mon Dec 19 15:41:51 2016
End time:	Mon Dec 19 15:57:28 2016

Host Information

Netbios Name:	IE10WIN7
IP:	192.168.108.15
MAC Address:	08:00:27:ff:21:6d
OS:	Microsoft Windows 7 Enterprise

Results Summary

Critical	High	Medium	Low	Info	Total
2	0	28	9	152	191

Results Details

0/icmp

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The ICMP timestamps seem to be in little endian format (not in network format)
The difference between the local and remote clocks is -203 seconds.
```

0/tcp

24786 - Nessus Windows Scan Not Performed with Admin Privileges

Synopsis

The Nessus scan of this host may be incomplete due to insufficient privileges provided.

Description

The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.

Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.
If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

Plugin Information:

Publication date: 2007/03/12, Modification date: 2013/01/07

Ports

tcp/0

```
It was not possible to connect to '\\IE10WIN7\ADMIN$' with the supplied credentials.
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

http://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2015/10/16

Ports

tcp/0

```
The following card manufacturers were identified :

08:00:27:ff:21:6d : PCS Systemtechnik GmbH
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2016/02/24

Ports

tcp/0

```
Remote operating system : Microsoft Windows 7 Enterprise
Confidence level : 99
Method : MSRPC

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

HTTP:Server: Microsoft-IIS/7.5
SMTP:!:220 localhost ESMTP server ready.
SSLcert:!:i/CN:localhosts/CN:localhost
b0238c547a905bfa119c4e8baccaeacf36491ff6
i/CN:IE10Win7s/CN:IE10Win7
32d6aeaa0431b35289b3896469df23bc60ecc216

RDP:000000000f0000001000010008000100090000000010010001000010


The remote host is running Microsoft Windows 7 Enterprise
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
```

```
Confidence level : 99
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/cpe.cfm

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2014/11/20

Ports

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_7:::enterprise

Following application CPE's matched on the remote system :

  cpe:/a:openssl:openssl:1.0.2h
  cpe:/a:apache:http_server:2.4.23
  cpe:/a:microsoft:iis:7.5 -> Microsoft Internet Information Services (IIS) 7.5
  cpe:/a:php:php:5.5.38
```

10919 - Open Port Re-check

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.
There are several possible reasons for this :
- The scan may have caused a service to freeze or stop running.
- An administrator may have stopped a particular service during the scanning process.
This might be an availability problem related to the following :
- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.
- This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.
- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.
In any case, the audit of the remote host might be incomplete and may need to be done again.

Solution

- Increase checks_read_timeout and/or reduce max_checks.
- Disable any IPS during the Nessus scan

Risk Factor

None

Plugin Information:

Publication date: 2002/03/19, Modification date: 2014/06/04

Ports
tcp/0

```
Port 9 was detected as being open but is now closed
Port 135 was detected as being open but is now closed
Port 110 was detected as being open but is now closed
Port 3389 was detected as being open but is now closed
Port 3306 was detected as being open but is now closed
Port 79 was detected as being open but is now closed
Port 2105 was detected as being open but is now closed
Port 80 was detected as being open but is now closed
Port 2107 was detected as being open but is now closed
Port 2224 was detected as being open but is now closed
Port 17 was detected as being open but is now closed
Port 81 was detected as being open but is now closed
Port 554 was detected as being open but is now closed
Port 7 was detected as being open but is now closed
Port 2103 was detected as being open but is now closed
Port 13 was detected as being open but is now closed
Port 19 was detected as being open but is now closed
Port 2869 was detected as being open but is now closed
Port 21 was detected as being open but is now closed
Port 143 was detected as being open but is now closed
Port 105 was detected as being open but is now closed
Port 106 was detected as being open but is now closed
Port 25 was detected as being open but is now closed
Port 443 was detected as being open but is now closed
```

66334 - Patch Report
Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information:

Publication date: 2013/07/08, Modification date: 2016/12/13

Ports
tcp/0

```
. You need to take the following 2 actions :

[ FileZilla Server < 0.9.31 Denial of Service (45112) ]

+ Action to take : Upgrade to FileZilla Server version 0.9.31 or later.


[ OpenSSL 1.0.2 < 1.0.2i Multiple Vulnerabilities (SWEET32) (93815) ]

+ Action to take : Upgrade to OpenSSL version 1.0.2i or later.

Note that the GOST ciphersuites vulnerability (VulnDB 144759) is not yet fixed by the vendor in
 an official release; however, a patch for the issue has been committed to the OpenSSL github
 repository.
```

19506 - Nessus Scan Information
Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2016/12/06

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.9.2
Plugin feed version : 201612162215
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : TestScan
Scanner IP : 192.168.108.88
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2016/12/19 15:41 SGT
Scan duration : 933 sec
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2013/04/11

Ports
udp/0

```
For your information, here is the traceroute from 192.168.108.88 to 192.168.108.15 :
192.168.108.88
192.168.108.15
```

7/tcp
11219 - Nessus SYN scanner
Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports
tcp/7

```
Port 7/tcp was found to be open
```

22964 - Service Detection
Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/11/03

Ports
tcp/7

```
An echo server is running on this port.
```

10061 - Echo Service Detection
Synopsis

An echo service is running on the remote host.

Description

The remote host is running the 'echo' service. This service echoes any data which is sent to it. This service is unused these days, so it is strongly advised that you disable it, as it may be used by attackers to set up denial of services attacks against this host.

Solution

- Under Unix systems, comment out the 'echo' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry key to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEcho HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEcho Then launch cmd.exe and type :

net stop simptcp net start simptcp To restart the service.

Risk Factor

None

References

CVE	CVE-1999-0103
CVE	CVE-1999-0635
XREF	OSVDB:150

Plugin Information:

Publication date: 1999/06/22, Modification date: 2014/06/09

Ports

tcp/7

7/udp

10061 - Echo Service Detection

Synopsis

An echo service is running on the remote host.

Description

The remote host is running the 'echo' service. This service echoes any data which is sent to it. This service is unused these days, so it is strongly advised that you disable it, as it may be used by attackers to set up denial of services attacks against this host.

Solution

- Under Unix systems, comment out the 'echo' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry key to 0 :
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEcho HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEcho Then launch cmd.exe and type :
net stop simptcp net start simptcp To restart the service.

Risk Factor

None

References

CVE	CVE-1999-0103
CVE	CVE-1999-0635
XREF	OSVDB:150

Plugin Information:

Publication date: 1999/06/22, Modification date: 2014/06/09

Ports

udp/7

9/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/9

```
Port 9/tcp was found to be open
```

11367 - Discard Service Detection

Synopsis

A discard service is running on the remote host.

Description

The remote host is running a 'discard' service. This service typically sets up a listening socket and will ignore all the data which it receives.
This service is unused these days, so it is advised that you disable it.

Solution

- Under Unix systems, comment out the 'discard' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry key to 0 :
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDiscard Then launch cmd.exe and type :
net stop simptcp net start simptcp To restart the service.

Risk Factor

None

Plugin Information:

Publication date: 2003/03/12, Modification date: 2011/03/11

Ports

tcp/9

13/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/13

```
Port 13/tcp was found to be open
```

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'
request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/11/18, Modification date: 2016/05/26

Ports

tcp/13

```
Daytime is running on this port.
```

10052 - Daytime Service Detection

Synopsis

A daytime service is running on the remote host.

Description

The remote host is running a 'daytime' service. This service is designed to give the local time of the day of this host to whoever connects to this port. The date format issued by this service may sometimes help an attacker to guess the operating system type of this host, or to set up timed authentication attacks against the remote host.
In addition, if the daytime service is running on a UDP port, an attacker may link it to the echo port of a third-party host using spoofing, thus creating a possible denial of service condition between this host and the third party.

Solution

- On Unix systems, comment out the 'daytime' line in /etc/inetd.conf and restart the inetd process.
- On Windows systems, set the following registry keys to 0 :
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime HKLM\System \CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime Next, launch cmd.exe and type :
net stop simptcp net start simptcp This will restart the service.

Risk Factor

None

Plugin Information:

Publication date: 1999/06/22, Modification date: 2014/05/09

Ports

tcp/13

13/udp

10052 - Daytime Service Detection

Synopsis

A daytime service is running on the remote host.

Description

The remote host is running a 'daytime' service. This service is designed to give the local time of the day of this host to whoever connects to this port. The date format issued by this service may sometimes help an attacker to guess the operating system type of this host, or to set up timed authentication attacks against the remote host.
In addition, if the daytime service is running on a UDP port, an attacker may link it to the echo port of a third-party host using spoofing, thus creating a possible denial of service condition between this host and the third party.

Solution

- On Unix systems, comment out the 'daytime' line in /etc/inetd.conf and restart the inetd process.
- On Windows systems, set the following registry keys to 0 :
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime HKLM\System \CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime Next, launch cmd.exe and type :
net stop simptcp net start simptcp This will restart the service.

Risk Factor

None

Plugin Information:

Publication date: 1999/06/22, Modification date: 2014/05/09

Ports

udp/13

17/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/17

```
Port 17/tcp was found to be open
```

17975 - Service Detection (GET request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/04/06, Modification date: 2016/07/20

Ports

tcp/17

```
qotd seems to be running on this port.
```

10198 - Quote of the Day (QOTD) Service Detection

Synopsis

The quote service (qotd) is running on this host.

Description

A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote.
Another quote of the day service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 17.
When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored).
An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution

- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry keys to 0 :
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd Then launch cmd.exe and type :
net stop simptcp net start simptcp To restart the service.

Risk Factor

None

References

CVE	CVE-1999-0103
XREF	OSVDB:150

Plugin Information:

Publication date: 1999/11/30, Modification date: 2011/07/26

Ports

tcp/17

17/udp

10198 - Quote of the Day (QOTD) Service Detection

Synopsis

The quote service (qotd) is running on this host.

Description

A server listens for TCP connections on TCP port 17. Once a connection is established a short message is sent out the connection (and any data received is thrown away). The service closes the connection after sending the quote.
Another quote of the day service is defined as a datagram based application on UDP. A server listens for UDP datagrams on UDP port 17.
When a datagram is received, an answering datagram is sent containing a quote (the data in the received datagram is ignored).
An easy attack is 'pingpong' which IP spoofs a packet between two machines running qotd. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

Solution

- Under Unix systems, comment out the 'qotd' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry keys to 0 :
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpQotd HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpQotd Then launch cmd.exe and type :
net stop simptcp net start simptcp To restart the service.

Risk Factor

None

References

CVE	CVE-1999-0103
XREF	OSVDB:150

Plugin Information:

Publication date: 1999/11/30, Modification date: 2011/07/26

Ports

udp/17

19/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/19

```
Port 19/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/11/03

Ports

tcp/19

```
A chargen server is running on this port.
```

19/udp

10043 - Chargen UDP Service Remote DoS

Synopsis

The remote host is running a 'chargen' service.

Description

When contacted, chargen responds with some random characters (something like all the characters in the alphabet in a row). When contacted via UDP, it will respond with a single UDP packet. When contacted via TCP, it will continue spewing characters until the client closes the connection.
The purpose of this service was to mostly test the TCP/IP protocol by itself, to make sure that all the packets were arriving at their destination unaltered. It is unused these days, so it is suggested you disable it, as an attacker may use it to set up an attack against this host, or against a third-party host using this host as a relay.
An easy attack is 'ping-pong' in which an attacker spoofs a packet between two machines running chargen. This will cause them to spew characters at each other, slowing the machines down and saturating the network.

See Also

http://www.nessus.org/u?f0dbdf05

Solution

- Under Unix systems, comment out the 'chargen' line in /etc/inetd.conf and restart the inetd process
- Under Windows systems, set the following registry keys to 0 :
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpChargen HKLM\System \CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpChargen
Then launch cmd.exe and type :
net stop simptcp net start simptcp
To restart the service.

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-1999-0103
XREF	OSVDB:150

Exploitable with

Metasploit (true)

Plugin Information:

Publication date: 1999/11/29, Modification date: 2014/04/23

Ports
udp/19

21/tcp
45112 - FileZilla Server < 0.9.31 Denial of Service

Synopsis
The remote FTP server is prone to a denial of service attack.

Description
According to its banner, the version of FileZilla Server installed on the remote host is older than version 0.9.31. An unspecified vulnerability in the SSL code for such versions can be exploited by a remote attacker to trigger a denial of service condition.

See Also
http://sourceforge.net/project/shownotes.php?release_id=665428

Solution
Upgrade to FileZilla Server version 0.9.31 or later.

Risk Factor
Medium

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

CVSS Temporal Score
4.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	34006
CVE	CVE-2009-0884
XREF	OSVDB:52698
XREF	Secunia:34089
XREF	CWE:119

Plugin Information:
Publication date: 2010/03/19, Modification date: 2016/05/05

Ports
tcp/21

```
The remote FileZilla server returned the following banner :

  FileZilla Server version 0.9.30 beta
```

11219 - Nessus SYN scanner

Synopsis
It is possible to determine which TCP ports are open.

Description
This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution
Protect your target with an IP filter.

Risk Factor
None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/21

```
Port 21/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/11/03

Ports

tcp/21

```
An FTP server is running on this port.
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2016/05/04

Ports

tcp/21

```
The remote FTP banner is :

220-FileZilla Server version 0.9.30 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
```

25/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/25

```
Port 25/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/11/03

Ports

tcp/25

```
An SMTP server is running on this port.
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.
Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/03/11

Ports

tcp/25

```
Remote SMTP server banner :

220 localhost ESMTP server ready.
```

79/tcp

10073 - Finger Recursive Request Arbitrary Site Redirection

Synopsis

It is possible to use the remote host to perform third-party host scans.

Description

The remote finger service accepts redirect requests. That is, users can perform requests like :
finger user@host@victim
This allows an attacker to use this computer as a relay to gather information on a third-party network. In addition, this type of syntax can be used to create a denial of service condition on the remote host.

Solution

Disable the remote finger daemon (comment out the 'finger' line in /etc/inetd.conf and restart the inetd process) or upgrade it to a more secure one.

Risk Factor

Medium

CVSS Base Score

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

References

CVE	CVE-1999-0105
CVE	CVE-1999-0106
XREF	OSVDB:64
XREF	OSVDB:5769

Plugin Information:

Publication date: 1999/06/22, Modification date: 2011/12/28

Ports

tcp/79

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/79

```
Port 79/tcp was found to be open
```

11154 - Unknown Service Detection: Banner Retrieval

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/11/18, Modification date: 2016/03/24

Ports

tcp/79

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

  Port   : 79
  Type   : get_http
  Banner :
0x00:  47 45 54 20 2F 20 48 54 54 50 2F 31 2E 30 20 69    GET / HTTP/1.0 i
          0x10:  73 20 6E 6F 74 20 6B 6E 6F 77 6E 20 61 74 20 74    s not known at t
          0x20:  68 69 73 20 73 69 74 65 2E 0D 0A                   his site...
```

80/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/80

```
Port 80/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/11/03

Ports

tcp/80

```
A web server is running on this port.
```

11422 - Web Server Unconfigured - Default Install Page Present

Synopsis

The remote web server is not configured or is improperly configured.

Description

The remote web server uses its default welcome page. Therefore, it's probable that this server is not used at all or is serving content that is meant to be hidden.

Solution

Disable this service if you do not use it.

Risk Factor

None

References

XREF OSVDB:3233

Plugin Information:

Publication date: 2003/03/20, Modification date: 2016/03/09

Ports

tcp/80

```
The default welcome page is from IIS.
```

49704 - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/10/04, Modification date: 2011/08/19

Ports

tcp/80

```
1 external URL was gathered on this web server :
URL...                                  - Seen on...


http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409 - /
```

50344 - Missing or Permissive Content-Security-Policy HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) response header or does not set one at all.
The CSP header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a properly configured Content-Security-Policy header for all requested resources.

Risk Factor

None

Plugin Information:

Publication date: 2010/10/26, Modification date: 2016/04/14

Ports

tcp/80

```
The following pages do not set a Content-Security-Policy response header or set a permissive
 policy:

  - http://192.168.108.15/
```

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.
The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

http://en.wikipedia.org/wiki/Clickjacking

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information:

Publication date: 2010/10/26, Modification date: 2016/04/14

Ports

tcp/80

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://192.168.108.15/
```

91815 - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/06/24, Modification date: 2016/06/24

Ports

tcp/80

```
The following sitemap was created from crawling linkable content on the target host :

  - http://192.168.108.15/

Attached is a copy of the sitemap file.
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/80

```
The remote web server type is :

Microsoft-IIS/7.5
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/12/10, Modification date: 2013/05/09

Ports

tcp/80

```
Based on the response to an OPTIONS request :

  - HTTP methods  GET  HEAD  POST  TRACE OPTIONS are allowed on :

    /


Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT CONNECT DEBUG GET HEAD INDEX LABEL
    MERGE MKACTIVITY MKWORKSPACE NOTIFY OPTIONS ORDERPATCH PATCH POLL
    POST REPORT RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE UNCHECKOUT
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /

  - Invalid/unknown HTTP methods are allowed on :

    /
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports

tcp/80

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : OPTIONS, TRACE, GET, HEAD, POST
Headers :

  Content-Type: text/html
  Last-Modified: Thu, 15 Dec 2016 06:25:17 GMT
  Accept-Ranges: bytes
  ETag: "caac919c56d21:0"
  Server: Microsoft-IIS/7.5
  Date: Mon, 19 Dec 2016 07:51:46 GMT
  Content-Length: 689
```

81/tcp

93815 - OpenSSL 1.0.2 < 1.0.2i Multiple Vulnerabilities (SWEET32)

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote host is running a version of OpenSSL 1.0.2 prior to 1.0.2i. It is, therefore, affected by the following vulnerabilities :
- Multiple integer overflow conditions exist in s3_srvr.c, ssl_sess.c, and t1_lib.c due to improper use of pointer arithmetic for heap-buffer boundary checks. An unauthenticated, remote attacker can exploit this to cause a denial of service. (CVE-2016-2177)
- An information disclosure vulnerability exists in the dsa_sign_setup() function in dsa_ossl.c due to a failure to properly ensure the use of constant-time operations.
An unauthenticated, remote attacker can exploit this, via a timing side-channel attack, to disclose DSA key information. (CVE-2016-2178)
- A denial of service vulnerability exists in the DTLS implementation due to a failure to properly restrict the lifetime of queue entries associated with unused out-of-order messages. An unauthenticated, remote attacker can exploit this, by maintaining multiple crafted DTLS sessions simultaneously, to exhaust memory.
(CVE-2016-2179)
- An out-of-bounds read error exists in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation. An unauthenticated, remote attacker can exploit this, via a crafted time-stamp file that is mishandled by the 'openssl ts' command, to cause denial of service or to disclose sensitive information.
(CVE-2016-2180)
- A denial of service vulnerability exists in the Anti-Replay feature in the DTLS implementation due to improper handling of epoch sequence numbers in records.
An unauthenticated, remote attacker can exploit this, via spoofed DTLS records, to cause legitimate packets to be dropped. (CVE-2016-2181)
- An overflow condition exists in the BN_bn2dec() function in bn_print.c due to improper validation of user-supplied input when handling BIGNUM values. An unauthenticated, remote attacker can exploit this to crash the process.
(CVE-2016-2182)
- A vulnerability exists, known as SWEET32, in the 3DES and Blowfish algorithms due to the use of weak 64-bit block ciphers by default. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.
(CVE-2016-2183)

- A flaw exists in the tls_decrypt_ticket() function in t1_lib.c due to improper handling of ticket HMAC digests. An unauthenticated, remote attacker can exploit this, via a ticket that is too short, to crash the process, resulting in a denial of service.
(CVE-2016-6302)
- An integer overflow condition exists in the MDC2_Update() function in mdc2dgst.c due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this to cause a heap-based buffer overflow, resulting in a denial of service condition or possibly the execution of arbitrary code.
(CVE-2016-6303)
- A flaw exists in the ssl_parse_clienthello_tlsext() function in t1_lib.c due to improper handling of overly large OCSP Status Request extensions from clients. An unauthenticated, remote attacker can exploit this, via large OCSP Status Request extensions, to exhaust memory resources, resulting in a denial of service condition.
(CVE-2016-6304)
- An out-of-bounds read error exists in the certificate parser that allows an unauthenticated, remote attacker to cause a denial of service via crafted certificate operations. (CVE-2016-6306)
- A flaw exists in the GOST ciphersuites due to the use of long-term keys to establish an encrypted connection. A man-in-the-middle attacker can exploit this, via a Key Compromise Impersonation (KCI) attack, to impersonate the server. (VulnDB 144759)

See Also

https://www.openssl.org/news/secadv/20160922.txt

http://www.nessus.org/u?09b29b30

https://sweet32.info/

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

Solution

Upgrade to OpenSSL version 1.0.2i or later.
Note that the GOST ciphersuites vulnerability (VulnDB 144759) is not yet fixed by the vendor in an official release; however, a patch for the issue has been committed to the OpenSSL github repository.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

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

CVSS Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	91081
BID	91319
BID	92117
BID	92557
BID	92628
BID	92630
BID	92982
BID	92984
BID	92987
BID	93150

BID	93153
CVE	CVE-2016-2177
CVE	CVE-2016-2178
CVE	CVE-2016-2179
CVE	CVE-2016-2180
CVE	CVE-2016-2181
CVE	CVE-2016-2182
CVE	CVE-2016-2183
CVE	CVE-2016-6302
CVE	CVE-2016-6303
CVE	CVE-2016-6304
CVE	CVE-2016-6306
XREF	OSVDB:139313
XREF	OSVDB:139471
XREF	OSVDB:142095
XREF	OSVDB:143021
XREF	OSVDB:143259
XREF	OSVDB:143309
XREF	OSVDB:143387
XREF	OSVDB:143388
XREF	OSVDB:143389
XREF	OSVDB:143392
XREF	OSVDB:144687
XREF	OSVDB:144688
XREF	OSVDB:144759

Plugin Information:

Publication date: 2016/09/30, Modification date: 2016/12/07

Ports

tcp/81

```
Banner           : Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38
Reported version : 1.0.2h
Fixed version    : 1.0.2i
```

46803 - PHP expose_php Information Disclosure

Synopsis

The configuration of PHP on the remote host allows disclosure of sensitive information.

Description

The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.
Other such Easter eggs likely exist, but Nessus has not checked for them.

See Also

http://www.0php.com/php_easter_egg.php

http://seclists.org/webappsec/2004/q4/324

Solution

In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

Risk Factor

Medium

CVSS Base Score

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

References

XREF OSVDB:12184

Plugin Information:

Publication date: 2010/06/03, Modification date: 2015/10/21

Ports

tcp/81

```
Nessus was able to verify the issue using the following URL :

  http://192.168.108.15:81/dashboard/phpinfo.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
```

10677 - Apache mod_status /server-status Information Disclosure

Synopsis

The remote web server discloses information about its status.

Description

It is possible to obtain an overview of the remote Apache web server's activity and performance by requesting the URL '/server-status'. This overview includes information such as current hosts and requests being processed, the number of workers idle and service requests, and CPU utilization.

Solution

If required, update Apache's configuration file(s) to either disable mod_status or ensure that access is limited to valid users / hosts.

Risk Factor

Medium

CVSS Base Score

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

References

XREF OSVDB:561

Plugin Information:

Publication date: 2001/05/28, Modification date: 2014/05/05

Ports

tcp/81

11213 - 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

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

CVSS Temporal Score

4.3 (CVSS2#E:H/RL:OF/RC:C)

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:5648
XREF	OSVDB:11408
XREF	OSVDB:50485
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information:

Publication date: 2003/01/23, Modification date: 2016/11/23

Ports

tcp/81

```
To disable these methods, add the following lines for each virtual
```

```
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus2055008460.html HTTP/1.1
Connection: Close
Host: 192.168.108.15
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Mon, 19 Dec 2016 07:51:45 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus2055008460.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.108.15
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

10678 - Apache mod_info /server-info Information Disclosure

Synopsis

The remote web server discloses information about its configuration.

Description

It is possible to obtain an overview of the remote Apache web server's configuration by requesting the URL '/server-info'. This overview includes information such as installed modules, their configuration, and assorted run-time settings.

See Also

http://httpd.apache.org/docs/mod/mod_info.html

Solution

If required, update Apache's configuration file(s) to either disable mod_info or ensure that access is limited to valid users / hosts.

Risk Factor

Medium

CVSS Base Score

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

References

XREF	OSVDB:562

Plugin Information:

Publication date: 2001/05/28, Modification date: 2013/01/25

Ports

tcp/81

40984 - Browsable Web Directories

Synopsis

Some directories on the remote web server are browsable.

Description

Miscellaneous Nessus plugins identified directories on this web server that are browsable.

See Also

http://www.nessus.org/u?0a35179e

Solution

Make sure that browsable directories do not leak confidential informative or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Publication date: 2009/09/15, Modification date: 2016/01/22

Ports

tcp/81

```
The following directories are browsable :

http://192.168.108.15:81/dashboard/docs/images/use-sqlite/
http://192.168.108.15:81/dashboard/docs/images/reset-mysql-password/
http://192.168.108.15:81/dashboard/docs/images/install-wordpress/
http://192.168.108.15:81/dashboard/docs/images/deploy-git-app/
http://192.168.108.15:81/dashboard/docs/images/create-framework-project-zf2/
http://192.168.108.15:81/dashboard/docs/images/create-framework-project-zf1/
http://192.168.108.15:81/dashboard/docs/
http://192.168.108.15:81/dashboard/images/team/
http://192.168.108.15:81/dashboard/images/stamps/
http://192.168.108.15:81/dashboard/images/screenshots/
http://192.168.108.15:81/dashboard/images/flags/
http://192.168.108.15:81/dashboard/images/blog/
http://192.168.108.15:81/xampp/
http://192.168.108.15:81/img/
http://192.168.108.15:81/dashboard/stylesheets/
http://192.168.108.15:81/dashboard/images/
http://192.168.108.15:81/dashboard/images/addons/
http://192.168.108.15:81/dashboard/docs/images/
http://192.168.108.15:81/dashboard/docs/images/access-phpmyadmin-remotely/
http://192.168.108.15:81/dashboard/docs/images/activate-use-xdebug/
http://192.168.108.15:81/dashboard/docs/images/backup-restore-mysql/
http://192.168.108.15:81/dashboard/docs/images/configure-vhosts/
http://192.168.108.15:81/dashboard/docs/images/configure-wildcard-subdomains/
http://192.168.108.15:81/dashboard/docs/images/send-mail/
http://192.168.108.15:81/dashboard/docs/images/transfer-files-ftp/
http://192.168.108.15:81/dashboard/docs/images/troubleshoot-apache/
http://192.168.108.15:81/dashboard/docs/images/use-different-php-version/
http://192.168.108.15:81/dashboard/docs/images/use-php-fcgi/
```

93112 - OpenSSL < 1.1.0 Default Weak 64-bit Block Cipher (SWEET32)

Synopsis

The service running on the remote host uses a weak encryption block cipher by default.

Description

According to its banner, the version of OpenSSL running on the remote host is prior to 1.1.0. It is, therefore, affected by a vulnerability, known as SWEET32, in the 3DES and Blowfish algorithms due to the use of weak 64-bit block ciphers by default. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a

'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info/

Solution

Upgrade to OpenSSL version 1.1.0 or later, and ensure all 64-bit block ciphers are disabled. Note that upgrading to OpenSSL 1.1.0 does not completely mitigate this vulnerability; it simply disables the vulnerable 64-bit block ciphers by default.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS Base Score

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

CVSS Temporal Score

2.5 (CVSS2#E:F/RL:ND/RC:ND)

References

BID	92630
CVE	CVE-2016-2183
XREF	OSVDB:143387
XREF	OSVDB:143388

Plugin Information:

Publication date: 2016/08/25, Modification date: 2016/12/07

Ports

tcp/81

```
Banner           : Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38
Reported version : 1.0.2h
Fixed version    : 1.1.0
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/81

```
Port 81/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/11/03

Ports

tcp/81

```
A web server is running on this port.
```

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/Predictable-Resource-Location

Solution

n/a

Risk Factor

None

References

XREF	OWASP:OWASP-CM-006

Plugin Information:

Publication date: 2002/06/26, Modification date: 2015/10/13

Ports

tcp/81

```
The following directories were discovered:
/cgi-bin, /error, /icons, /img, /server-info, /server-status, /xampp

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

10662 - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.
It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/05/04, Modification date: 2016/12/08

Ports

tcp/81

```
Webmirror performed 288 queries in 12s (24.000 queries per second)

The following CGIs have been discovered :


+ CGI : /
  Methods : GET
  Argument :
   Value: util_ldap.c

Directory index found at /xampp/
Directory index found at /img/
Directory index found at /dashboard/stylesheets/
Directory index found at /dashboard/images/
Directory index found at /dashboard/images/addons/
Directory index found at /dashboard/images/blog/
Directory index found at /dashboard/images/flags/
Directory index found at /dashboard/images/screenshots/
Directory index found at /dashboard/images/stamps/
Directory index found at /dashboard/images/team/
Directory index found at /dashboard/docs/
Directory index found at /dashboard/docs/images/
Directory index found at /dashboard/docs/images/access-phpmyadmin-remotely/
Directory index found at /dashboard/docs/images/activate-use-xdebug/
Directory index found at /dashboard/docs/images/backup-restore-mysql/
Directory index found at /dashboard/docs/images/configure-vhosts/
Directory index found at /dashboard/docs/images/configure-wildcard-subdomains/
Directory index found at /dashboard/docs/images/create-framework-project-zf1/
Directory index found at /dashboard/docs/images/create-framework-project-zf2/
Directory index found at /dashboard/docs/images/deploy-git-app/
Directory index found at /dashboard/docs/images/install-wordpress/
Directory index found at /dashboard/docs/images/reset-mysql-password/
Directory index found at /dashboard/docs/images/send-mail/
Directory index found at /dashboard/docs/images/transfer-files-ftp/
Directory index found at /dashboard/docs/images/troubleshoot-apache/
Directory index found at /dashboard/docs/images/use-different-php-version/
Directory index found at /dashboard/docs/images/use-php-fcgi/
Directory index found at /dashboard/docs/images/use-sqlite/

Extraneous phpinfo() script found at /dashboard/phpinfo.php
```

49704 - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/10/04, Modification date: 2011/08/19

Ports

tcp/81

```
73 external URLs were gathered on this web server :
URL...                                  - Seen on...
```

```
http://app01.localhost                  - /dashboard/docs/configure-vhosts.html
http://app02.localhost                  - /dashboard/docs/configure-vhosts.html
http://bitnami.com/stack/xampp?utm_source=bitnami&utm_medium=installer&utm_campaign=XAMPP%2BModule
 - /dashboard/
http://cdnjs.cloudflare.com/ajax/libs/font-awesome/3.1.0/css/font-awesome.min.css - /dashboard/
http://client1/                         - /dashboard/docs/configure-vhosts.html
http://client2/                         - /dashboard/docs/configure-vhosts.html
http://code.google.com/p/gitextensions/ - /dashboard/docs/deploy-git-app.html
http://framework.zend.com/              - /dashboard/docs/create-framework-project-zf1.html
http://framework.zend.com/downloads/latest - /dashboard/docs/create-framework-project-zf1.html
http://framework.zend.com/manual/1.12/en/learning.html - /dashboard/docs/create-framework-project-
zf1.html
http://framework.zend.com/manual/2.3/en/user-guide/overview.html - /dashboard/docs/create-
framework-project-zf2.html
http://git-extensions-documentation.readthedocs.org/en/latest/getting_started.html - /dashboard/
docs/deploy-git-app.html
http://git-scm.com/                     - /dashboard/docs/deploy-git-app.html
http://git-scm.com/book                 - /dashboard/docs/deploy-git-app.html
http://git-scm.com/download/win         - /dashboard/docs/create-framework-project-zf2.html
http://localhost                        - /dashboard/docs/install-wordpress.html
http://localhost/Slim                   - /dashboard/docs/deploy-git-app.html
http://localhost/example.php            - /dashboard/docs/transfer-files-ftp.html
http://localhost/example/phpmailer.php  - /dashboard/docs/send-mail.html
http://localhost/myapp                  - /dashboard/docs/create-framework-project-zf1.html
http://localhost/myapp/                 - /dashboard/docs/create-framework-project-zf1.html
http://localhost/phpMyAdmin             - /dashboard/do [...]
```

50344 - Missing or Permissive Content-Security-Policy HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) response header or does not set one at all.
The CSP header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a properly configured Content-Security-Policy header for all requested resources.

Risk Factor

None

Plugin Information:

Publication date: 2010/10/26, Modification date: 2016/04/14

Ports

tcp/81

```
The following pages do not set a Content-Security-Policy response header or set a permissive
 policy:

  - http://192.168.108.15:81/applications.html
  - http://192.168.108.15:81/dashboard/
  - http://192.168.108.15:81/dashboard/docs/
  - http://192.168.108.15:81/dashboard/docs/access-phpmyadmin-remotely.html
  - http://192.168.108.15:81/dashboard/docs/activate-use-xdebug.html
  - http://192.168.108.15:81/dashboard/docs/backup-restore-mysql.html
  - http://192.168.108.15:81/dashboard/docs/change-mysql-temp-dir.html
  - http://192.168.108.15:81/dashboard/docs/configure-vhosts.html
  - http://192.168.108.15:81/dashboard/docs/configure-wildcard-subdomains.html
  - http://192.168.108.15:81/dashboard/docs/create-framework-project-zf1.html
  - http://192.168.108.15:81/dashboard/docs/create-framework-project-zf2.html
  - http://192.168.108.15:81/dashboard/docs/deploy-git-app.html
  - http://192.168.108.15:81/dashboard/docs/images/
```

```
- http://192.168.108.15:81/dashboard/docs/images/access-phpmyadmin-remotely/
- http://192.168.108.15:81/dashboard/docs/images/activate-use-xdebug/
- http://192.168.108.15:81/dashboard/docs/images/backup-restore-mysql/
- http://192.168.108.15:81/dashboard/docs/images/configure-vhosts/
- http://192.168.108.15:81/dashboard/docs/images/configure-wildcard-subdomains/
- http://192.168.108.15:81/dashboard/docs/images/create-framework-project-zf1/
- http://192.168.108.15:81/dashboard/docs/images/create-framework-project-zf2/
- http://192.168.108.15:81/dashboard/docs/images/deploy-git-app/
- http://192.168.108.15:81/dashboard/docs/images/install-wordpress/
- http://192.168.108.15:81/dashboard/docs/images/reset-mysql-password/
- http://192.168.108.15:81/dashboard/docs/images/send-mail/
- http://192.168.108.15:81/dashboard/docs/images/transfer-files-ftp/
- http://192.168.108.15:81/dashboard/docs/images/troubleshoot-apache/
- http://192.168.108.15:81/dashboard/docs/images/use-different-php-version/
- http://192.168.108.15:81/dashboard/docs/images/use-php-fcgi/
- http://192.1 [...]
```

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.
The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

http://en.wikipedia.org/wiki/Clickjacking

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information:

Publication date: 2010/10/26, Modification date: 2016/04/14

Ports

tcp/81

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://192.168.108.15:81/applications.html
  - http://192.168.108.15:81/dashboard/
  - http://192.168.108.15:81/dashboard/docs/
  - http://192.168.108.15:81/dashboard/docs/access-phpmyadmin-remotely.html
  - http://192.168.108.15:81/dashboard/docs/activate-use-xdebug.html
  - http://192.168.108.15:81/dashboard/docs/backup-restore-mysql.html
  - http://192.168.108.15:81/dashboard/docs/change-mysql-temp-dir.html
  - http://192.168.108.15:81/dashboard/docs/configure-vhosts.html
  - http://192.168.108.15:81/dashboard/docs/configure-wildcard-subdomains.html
  - http://192.168.108.15:81/dashboard/docs/create-framework-project-zf1.html
  - http://192.168.108.15:81/dashboard/docs/create-framework-project-zf2.html
  - http://192.168.108.15:81/dashboard/docs/deploy-git-app.html
  - http://192.168.108.15:81/dashboard/docs/images/
  - http://192.168.108.15:81/dashboard/docs/images/access-phpmyadmin-remotely/
  - http://192.168.108.15:81/dashboard/docs/images/activate-use-xdebug/
  - http://192.168.108.15:81/dashboard/docs/images/backup-restore-mysql/
  - http://192.168.108.15:81/dashboard/docs/images/configure-vhosts/
  - http://192.168.108.15:81/dashboard/docs/images/configure-wildcard-subdomains/
  - http://192.168.108.15:81/dashboard/docs/images/create-framework-project-zf1/
  - http://192.168.108.15:81/dashboard/docs/images/create-framework-project-zf2/
  - http://192.168.108.15:81/dashboard/docs/images/deploy-git-app/
  - http://192.168.108.15:81/dashboard/docs/images/install-wordpress/
  - http://192.168.108.15:81/dashboard/docs/images/reset-mysql-password/
  - http://192.168.108.15:81/dashboard/docs/images/send-mail/
  - http://192.168.108.15:81/dashboard/docs/images/transfer-files-ftp/
```

```
  - http://192.168.108.15:81/dashboard/docs/images/troubleshoot-apache/
  - http://192.168.108.15:81/dashboard/docs/images/use-different-php-version/
  - http://192.168.108.15:81/dashboard/docs/images/use-php-fcgi/
  - http://192.168.108.1 [...]
```

91815 - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/06/24, Modification date: 2016/06/24

Ports

tcp/81

```
The following sitemap was created from crawling linkable content on the target host :

  - http://192.168.108.15:81/applications.html
  - http://192.168.108.15:81/bitnami.css
  - http://192.168.108.15:81/dashboard/
  - http://192.168.108.15:81/dashboard/docs/
  - http://192.168.108.15:81/dashboard/docs/access-phpmyadmin-remotely.html
  - http://192.168.108.15:81/dashboard/docs/access-phpmyadmin-remotely.pdf
  - http://192.168.108.15:81/dashboard/docs/activate-use-xdebug.html
  - http://192.168.108.15:81/dashboard/docs/activate-use-xdebug.pdf
  - http://192.168.108.15:81/dashboard/docs/activate-use-xdebug.pdfmarks
  - http://192.168.108.15:81/dashboard/docs/backup-restore-mysql.html
  - http://192.168.108.15:81/dashboard/docs/backup-restore-mysql.pdf
  - http://192.168.108.15:81/dashboard/docs/backup-restore-mysql.pdfmarks
  - http://192.168.108.15:81/dashboard/docs/change-mysql-temp-dir.html
  - http://192.168.108.15:81/dashboard/docs/change-mysql-temp-dir.pdf
  - http://192.168.108.15:81/dashboard/docs/change-mysql-temp-dir.pdfmarks
  - http://192.168.108.15:81/dashboard/docs/configure-vhosts.html
  - http://192.168.108.15:81/dashboard/docs/configure-vhosts.pdf
  - http://192.168.108.15:81/dashboard/docs/configure-vhosts.pdfmarks
  - http://192.168.108.15:81/dashboard/docs/configure-wildcard-subdomains.html
  - http://192.168.108.15:81/dashboard/docs/configure-wildcard-subdomains.pdf
  - http://192.168.108.15:81/dashboard/docs/configure-wildcard-subdomains.pdfmarks
  - http://192.168.108.15:81/dashboard/docs/create-framework-project-zf1.html
  - http://192.168.108.15:81/dashboard/docs/create-framework-project-zf1.pdf
  - http://192.168.108.15:81/dashboard/docs/create-framework-project-zf1.pdfmarks
  - http://192.168.108.15:81/dashboard/docs/create-framework-project-zf2.html
  - http://192.168.108.15:81/dashboard/docs/create-framework-project-zf2.pdf
  - http://192.168.108.15:81/dashboard/docs/create-framework-project-zf2.pdfmarks
  - http://192.168.108.15:81/dashboard/docs/deploy-git-app.html
  - http://192.168. [...]
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/81

```
The remote web server type is :

Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.
```

57323 - OpenSSL Version Detection

Synopsis

Nessus was able to detect the OpenSSL version.

Description

Nessus was able to extract the OpenSSL version from the web server's banner. Note that security patches in many cases are backported and the displayed version number does not show the patch level. Using it to identify vulnerable software is likely to lead to false detections.

See Also

http://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/16, Modification date: 2016/11/18

Ports

tcp/81

```
  Source              : Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38
  Reported version    : 1.0.2h
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/12/10, Modification date: 2013/05/09

Ports

tcp/81

```
Based on the response to an OPTIONS request :
```

```
  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /dashboard
    /dashboard/docs
    /dashboard/docs/images
    /dashboard/docs/images/access-phpmyadmin-remotely
    /dashboard/docs/images/activate-use-xdebug
    /dashboard/docs/images/backup-restore-mysql
    /dashboard/docs/images/configure-vhosts
    /dashboard/docs/images/configure-wildcard-subdomains
    /dashboard/docs/images/create-framework-project-zf1
    /dashboard/docs/images/create-framework-project-zf2
    /dashboard/docs/images/deploy-git-app
    /dashboard/docs/images/install-wordpress
    /dashboard/docs/images/reset-mysql-password
    /dashboard/docs/images/send-mail
    /dashboard/docs/images/transfer-files-ftp
    /dashboard/docs/images/troubleshoot-apache
    /error
    /icons
    /img
    /server-info
    /server-status
    /xampp


Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
    LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
    ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /cgi-bin

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /
    /dashboard
    /dashboard/docs
    /dashboard/docs/images
    /dashboard/docs/images/access-phpmyadmin-remotely
    /dashboard/docs/images/activate-use-xdebug
    /dashboard/docs/images/backup-restore-mysql
    /dashboard/docs/images/configure-vhosts
    /dashboard/docs/images/configure-wildcard-subdomains
    /dashboard/docs/images/create-framework-project-zf1
    /dashboard/docs/images/create-framework-project-zf2
    /dashboard/docs/images/deploy-git-app
    /dashboard/docs/images/install-wordpress
    /dashboard/docs/images/reset-mysql-password
    /dashboard/docs/images/send-mail
    /dashboard/docs/images/transfer-files-ft [...]
```

48243 - PHP Version

Synopsis

It is possible to obtain the version number of the remote PHP install.

Description

This plugin attempts to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/08/04, Modification date: 2014/10/31

Ports

tcp/81

```
Nessus was able to identify the following PHP version information :

  Version : 5.5.38
  Source  : Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports

tcp/81

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Mon, 19 Dec 2016 07:51:46 GMT
  Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38
  X-Powered-By: PHP/5.5.38
  Location: http://192.168.108.15:81/dashboard/
  Content-Length: 0
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html
```

91634 - HyperText Transfer Protocol (HTTP) Redirect Information

Synopsis

The remote web server redirects requests to the root directory.

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.
This plugin is informational only and does not denote a security problem.

Solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

Risk Factor

None

Plugin Information:

Publication date: 2016/06/16, Modification date: 2016/06/16

Ports

tcp/81

```
  Request         : http://192.168.108.15:81/
  HTTP response   : HTTP/1.1 302 Found
  Redirect to     : http://192.168.108.15:81/dashboard/
  Redirect type   : 30x redirect
```

```
Final page      : http://192.168.108.15:81/dashboard/
HTTP response   : HTTP/1.1 200 OK
```

33817 - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.
The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.
Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/10/26, Modification date: 2014/03/12

Ports

tcp/81

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

directory traversal (extended test)      : S=0          SP=0         AP=0         SC=0
 AC=0
arbitrary command execution (time based) : S=0          SP=0         AP=0         SC=0
 AC=0
web code injection                       : S=0          SP=0         AP=0         SC=0
 AC=0
unseen parameters                        : S=0          SP=0         AP=0         SC=0
 AC=0
directory traversal (write access)       : S=0          SP=0         AP=0         SC=0
 AC=0
arbitrary command execution              : S=0          SP=0         AP=0         SC=0
 AC=0
SSI injection                            : S=0          SP=0         AP=0         SC=0
 AC=0
local file inclusion                     : S=0          SP=0         AP=0         SC=0
 AC=0
SQL injection (2nd order)                : S=0          SP=0         AP=0         SC=0
 AC=0
directory traversal                      : S=0          SP=0         AP=0         SC=0
 AC=0
cross-site scripting (comprehensive test): S=0          SP=0         AP=0         SC=0
 AC=0
SQL injection                            : S=0          SP=0         AP=0         SC=0
 AC=0
persistent XSS                           : S=0          SP=0         AP=0         SC=0
 AC=0
format string                            : S=0          SP=0         AP=0         SC=0
 AC=0
blind SQL injection (4 requests)         : S=0          SP=0         AP=0         SC=0
 AC=0
XML injection                            : S=0          SP=0         AP=0         SC=0
 AC=0
blind SQL injection                      : S=0          SP=0         AP=0         SC=0
 AC=0
injectable parameter                   [...]
```

11419 - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

None

Plugin Information:

Publication date: 2003/03/19, Modification date: 2013/08/13

Ports

tcp/81

```
The following office-related files are available on the remote server :

  - Adobe Acrobat files (.pdf) :
    /dashboard/docs/use-sqlite.pdf
    /dashboard/docs/install-wordpress.pdf
    /dashboard/docs/increase-php-file-upload-limit.pdf
    /dashboard/docs/deploy-git-app.pdf
    /dashboard/docs/create-framework-project-zf2.pdf
    /dashboard/docs/create-framework-project-zf1.pdf
    /dashboard/docs/configure-wildcard-subdomains.pdf
    /dashboard/docs/access-phpmyadmin-remotely.pdf
    /dashboard/docs/activate-use-xdebug.pdf
    /dashboard/docs/backup-restore-mysql.pdf
    /dashboard/docs/change-mysql-temp-dir.pdf
    /dashboard/docs/configure-vhosts.pdf
    /dashboard/docs/reset-mysql-password.pdf
    /dashboard/docs/send-mail.pdf
    /dashboard/docs/transfer-files-ftp.pdf
    /dashboard/docs/troubleshoot-apache.pdf
    /dashboard/docs/use-different-php-version.pdf
    /dashboard/docs/use-php-fcgi.pdf
```

40406 - CGI Generic Tests HTTP Errors

Synopsis

Nessus encountered errors while running its generic CGI attacks.

Description

Nessus ran into trouble while running its generic CGI tests against the remote web server (for example, connection refused, timeout, etc). When this happens, Nessus aborts the current test and switches to the next CGI script on the same port or to another web server. Thus, test results may be incomplete.

Solution

Rescan with a longer network timeout or less parallelism for example, by changing the following options in the scan policy :
- Network -> Network Receive Timeout (check_read_timeout)
- Options -> Number of hosts in parallel (max_hosts)
- Options -> Number of checks in parallel (max_checks)

Risk Factor

None

Plugin Information:

Publication date: 2009/07/28, Modification date: 2011/09/21

Ports

tcp/81

```
Nessus encountered :

  - 3 errors involving SSI injection (on HTTP headers) checks :
   . connecting to server: errno=6 (connection refused)
  - 1 error involving SQL injection (on HTTP headers) checks :
   . reading the status line: errno=2 (connection reset by peer)
```

```
  - 1 error involving XSS (on HTTP headers) checks :
   . reading the status line: errno=2 (connection reset by peer)

This web server appears to be unresponsive now.
```

105/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/105

```
Port 105/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/11/03

Ports

tcp/105

```
A ph server is running on this port.
```

106/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports
tcp/106

```
Port 106/tcp was found to be open
```

110/tcp
15855 - POP3 Cleartext Logins Permitted
Synopsis

The remote POP3 daemon allows credentials to be transmitted in cleartext.

Description

The remote host is running a POP3 daemon that allows cleartext logins over unencrypted connections. An attacker can uncover user names and passwords by sniffing traffic to the POP3 daemon if a less secure authentication mechanism (eg, USER command, AUTH PLAIN, AUTH LOGIN) is used.

See Also

http://tools.ietf.org/html/rfc2222

http://tools.ietf.org/html/rfc2595

Solution

Contact your vendor for a fix or encrypt traffic with SSL / TLS using stunnel.

Risk Factor

Low

CVSS Base Score

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

Plugin Information:

Publication date: 2004/11/30, Modification date: 2016/11/23

Ports
tcp/110

```
The following cleartext methods are supported :
USER
```

11219 - Nessus SYN scanner
Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports
tcp/110

```
Port 110/tcp was found to be open
```

22964 - Service Detection
Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/11/03

Ports

tcp/110

```
A POP3 server is running on this port.
```

10185 - POP Server Detection

Synopsis

A POP server is listening on the remote port.

Description

The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.

See Also

http://en.wikipedia.org/wiki/Post_Office_Protocol

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/03/11

Ports

tcp/110

```
Remote POP server banner :

+OK <245261337.17473@localhost>, POP3 server ready.
```

135/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/135

```
The following DCERPC services are available locally :
```

```
Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0528C0

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0528C0

Object UUID : 6d726574-7273-0076-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-b15022c9c89b337169

Object UUID : 52ef130c-08fd-4388-86b3-6edf00000001
UUID : 12e65dd8-887f-41ef-91bf-8d816c42c2e7, version 1.0
Description : Unknown RPC service
Annotation : Secure Desktop LRPC interface
Type : Local RPC service
Named pipe : WMsgKRpc052181

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000001
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc052181

Object UUID : 73757274-6574-6964-6e73-74616c6c6572
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : OLEA9D5B9D69D434182AB9168E8933A

Object UUID : 73757274-6574-6964-6e73-74616c6c6572
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-30d0e690d0dc9e30a6

Object UUID : 00000000-0000-0000-0000-000000000000
UU [...]
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/135

```
Port 135/tcp was found to be open
```

137/udp

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests. Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2016/02/26

Ports

udp/137

```
The following 6 NetBIOS names have been gathered :

 IE10WIN7         = File Server Service
 IE10WIN7         = Computer name
 WORKGROUP        = Workgroup / Domain name
 WORKGROUP        = Browser Service Elections
 WORKGROUP        = Master Browser
 __MSBROWSE__     = Master Browser

The remote host has the following MAC address on its adapter :

   08:00:27:ff:21:6d
```

139/tcp

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/139

```
An SMB server is running on this port.
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/139

```
Port 139/tcp was found to be open
```

143/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/143

```
Port 143/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/11/03

Ports

tcp/143

```
An IMAP server is running on this port.
```

11414 - IMAP Service Banner Retrieval

Synopsis

An IMAP server is running on the remote host.

Description

An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/03/18, Modification date: 2011/03/16

Ports

tcp/143

```
The remote imap server banner is :

* OK localhost IMAP4rev1 Mercury/32 v4.62 server ready.
```

443/tcp

93815 - OpenSSL 1.0.2 < 1.0.2i Multiple Vulnerabilities (SWEET32)

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

According to its banner, the remote host is running a version of OpenSSL 1.0.2 prior to 1.0.2i. It is, therefore, affected by the following vulnerabilities :
- Multiple integer overflow conditions exist in s3_srvr.c, ssl_sess.c, and t1_lib.c due to improper use of pointer arithmetic for heap-buffer boundary checks. An unauthenticated, remote attacker can exploit this to cause a denial of service. (CVE-2016-2177)
- An information disclosure vulnerability exists in the dsa_sign_setup() function in dsa_ossl.c due to a failure to properly ensure the use of constant-time operations.
An unauthenticated, remote attacker can exploit this, via a timing side-channel attack, to disclose DSA key information. (CVE-2016-2178)
- A denial of service vulnerability exists in the DTLS implementation due to a failure to properly restrict the lifetime of queue entries associated with unused out-of-order messages. An unauthenticated, remote attacker can exploit this, by maintaining multiple crafted DTLS sessions simultaneously, to exhaust memory.
(CVE-2016-2179)
- An out-of-bounds read error exists in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation. An unauthenticated, remote attacker can exploit this, via a crafted time-stamp file that is mishandled by the 'openssl ts' command, to cause denial of service or to disclose sensitive information.
(CVE-2016-2180)
- A denial of service vulnerability exists in the Anti-Replay feature in the DTLS implementation due to improper handling of epoch sequence numbers in records.
An unauthenticated, remote attacker can exploit this, via spoofed DTLS records, to cause legitimate packets to be dropped. (CVE-2016-2181)
- An overflow condition exists in the BN_bn2dec() function in bn_print.c due to improper validation of user-supplied input when handling BIGNUM values. An unauthenticated, remote attacker can exploit this to crash the process.
(CVE-2016-2182)
- A vulnerability exists, known as SWEET32, in the 3DES and Blowfish algorithms due to the use of weak 64-bit block ciphers by default. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.
(CVE-2016-2183)
- A flaw exists in the tls_decrypt_ticket() function in t1_lib.c due to improper handling of ticket HMAC digests. An unauthenticated, remote attacker can exploit this, via a ticket that is too short, to crash the process, resulting in a denial of service.
(CVE-2016-6302)
- An integer overflow condition exists in the MDC2_Update() function in mdc2dgst.c due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this to cause a heap-based buffer overflow, resulting in a denial of service condition or possibly the execution of arbitrary code.
(CVE-2016-6303)

- A flaw exists in the ssl_parse_clienthello_tlsext() function in t1_lib.c due to improper handling of overly large OCSP Status Request extensions from clients. An unauthenticated, remote attacker can exploit this, via large OCSP Status Request extensions, to exhaust memory resources, resulting in a denial of service condition. (CVE-2016-6304)
- An out-of-bounds read error exists in the certificate parser that allows an unauthenticated, remote attacker to cause a denial of service via crafted certificate operations. (CVE-2016-6306)
- A flaw exists in the GOST ciphersuites due to the use of long-term keys to establish an encrypted connection. A man-in-the-middle attacker can exploit this, via a Key Compromise Impersonation (KCI) attack, to impersonate the server. (VulnDB 144759)

See Also

https://www.openssl.org/news/secadv/20160922.txt

http://www.nessus.org/u?09b29b30

https://sweet32.info/

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

Solution

Upgrade to OpenSSL version 1.0.2i or later.
Note that the GOST ciphersuites vulnerability (VulnDB 144759) is not yet fixed by the vendor in an official release; however, a patch for the issue has been committed to the OpenSSL github repository.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

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

CVSS Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:ND)

References

BID	91081
BID	91319
BID	92117
BID	92557
BID	92628
BID	92630
BID	92982
BID	92984
BID	92987
BID	93150
BID	93153
CVE	CVE-2016-2177
CVE	CVE-2016-2178
CVE	CVE-2016-2179

CVE	CVE-2016-2180
CVE	CVE-2016-2181
CVE	CVE-2016-2182
CVE	CVE-2016-2183
CVE	CVE-2016-6302
CVE	CVE-2016-6303
CVE	CVE-2016-6304
CVE	CVE-2016-6306
XREF	OSVDB:139313
XREF	OSVDB:139471
XREF	OSVDB:142095
XREF	OSVDB:143021
XREF	OSVDB:143259
XREF	OSVDB:143309
XREF	OSVDB:143387
XREF	OSVDB:143388
XREF	OSVDB:143389
XREF	OSVDB:143392
XREF	OSVDB:144687
XREF	OSVDB:144688
XREF	OSVDB:144759

Plugin Information:

Publication date: 2016/09/30, Modification date: 2016/12/07

Ports

tcp/443

```
Banner           : Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38
Reported version : 1.0.2h
Fixed version    : 1.0.2i
```

51192 - 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 unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

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)

Plugin Information:

Publication date: 2010/12/15, Modification date: 2015/10/21

Ports

tcp/443

```
The following certificate was at the top of the certificate
chain sent by the remote host, but is signed by an unknown
certificate authority :

|-Subject : CN=localhost
|-Issuer  : CN=localhost
```

35291 - 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 (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.
Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.
Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

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)

References

BID	11849

BID	33065
CVE	CVE-2004-2761
XREF	OSVDB:45106
XREF	OSVDB:45108
XREF	OSVDB:45127
XREF	CERT:836068
XREF	CWE:310

Plugin Information:

Publication date: 2009/01/05, Modification date: 2016/09/19

Ports

tcp/443

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

|-Subject             : CN=localhost
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Nov 10 23:48:47 2009 GMT
|-Valid To            : Nov 08 23:48:47 2019 GMT
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

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)

Plugin Information:

Publication date: 2012/01/17, Modification date: 2016/12/14

Ports

tcp/443

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=localhost
```

42873 - 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)

Plugin Information:

Publication date: 2009/11/23, Modification date: 2015/10/21

Ports

tcp/443

```
Here is the list of medium strength SSL ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key)

    TLSv1
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      ECDHE-RSA-DES-CBC3-SHA       Kx=ECDH        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

45411 - 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)

Plugin Information:

Publication date: 2010/04/03, Modification date: 2014/03/11

Ports

tcp/443

```
The identities known by Nessus are :

  192.168.108.15
  192.168.108.15

The Common Name in the certificate is :

  localhost
```

46803 - PHP expose_php Information Disclosure

Synopsis

The configuration of PHP on the remote host allows disclosure of sensitive information.

Description

The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.
Other such Easter eggs likely exist, but Nessus has not checked for them.

See Also

http://www.0php.com/php_easter_egg.php

http://seclists.org/webappsec/2004/q4/324

Solution

In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

Risk Factor

Medium

CVSS Base Score

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

References

XREF	OSVDB:12184

Plugin Information:

Publication date: 2010/06/03, Modification date: 2015/10/21

Ports

tcp/443

```
Nessus was able to verify the issue using the following URL :

  https://192.168.108.15/dashboard/phpinfo.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
```

10677 - Apache mod_status /server-status Information Disclosure

Synopsis

The remote web server discloses information about its status.

Description

It is possible to obtain an overview of the remote Apache web server's activity and performance by requesting the URL '/server-status'. This overview includes information such as current hosts and requests being processed, the number of workers idle and service requests, and CPU utilization.

Solution

If required, update Apache's configuration file(s) to either disable mod_status or ensure that access is limited to valid users / hosts.

Risk Factor

Medium

CVSS Base Score

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

References

XREF	OSVDB:561

Plugin Information:

Publication date: 2001/05/28, Modification date: 2014/05/05

Ports

tcp/443

11213 - 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

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

CVSS Temporal Score

4.3 (CVSS2#E:H/RL:OF/RC:C)

References

BID	9506
BID	9561
BID	11604
BID	33374
BID	37995
CVE	CVE-2003-1567
CVE	CVE-2004-2320
CVE	CVE-2010-0386
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:5648
XREF	OSVDB:11408
XREF	OSVDB:50485
XREF	CERT:288308
XREF	CERT:867593
XREF	CWE:16
XREF	CWE:200

Plugin Information:

Publication date: 2003/01/23, Modification date: 2016/11/23

Ports

tcp/443

```
To disable these methods, add the following lines for each virtual
host in your configuration file :

    RewriteEngine on
    RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
    RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus1508038558.html HTTP/1.1
Connection: Close
Host: 192.168.108.15
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Mon, 19 Dec 2016 07:51:45 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus1508038558.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.108.15
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

10678 - Apache mod_info /server-info Information Disclosure

Synopsis

The remote web server discloses information about its configuration.

Description

It is possible to obtain an overview of the remote Apache web server's configuration by requesting the URL '/server-info'. This overview includes information such as installed modules, their configuration, and assorted run-time settings.

See Also

http://httpd.apache.org/docs/mod/mod_info.html

Solution

If required, update Apache's configuration file(s) to either disable mod_info or ensure that access is limited to valid users / hosts.

Risk Factor

Medium

CVSS Base Score

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

References

XREF OSVDB:562

Plugin Information:

Publication date: 2001/05/28, Modification date: 2013/01/25

Ports

tcp/443

40984 - Browsable Web Directories

Synopsis

Some directories on the remote web server are browsable.

Description

Miscellaneous Nessus plugins identified directories on this web server that are browsable.

See Also

http://www.nessus.org/u?0a35179e

Solution

Make sure that browsable directories do not leak confidential informative or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Publication date: 2009/09/15, Modification date: 2016/01/22

Ports

tcp/443

```
The following directories are browsable :

https://192.168.108.15/dashboard/docs/images/use-sqlite/
https://192.168.108.15/dashboard/docs/images/reset-mysql-password/
https://192.168.108.15/dashboard/docs/images/install-wordpress/
https://192.168.108.15/dashboard/docs/images/deploy-git-app/
https://192.168.108.15/dashboard/docs/images/create-framework-project-zf2/
https://192.168.108.15/dashboard/docs/images/create-framework-project-zf1/
https://192.168.108.15/dashboard/docs/
https://192.168.108.15/dashboard/images/team/
https://192.168.108.15/dashboard/images/stamps/
https://192.168.108.15/dashboard/images/screenshots/
https://192.168.108.15/dashboard/images/flags/
https://192.168.108.15/dashboard/images/blog/
https://192.168.108.15/xampp/
https://192.168.108.15/img/
https://192.168.108.15/dashboard/stylesheets/
https://192.168.108.15/dashboard/images/
https://192.168.108.15/dashboard/images/addons/
https://192.168.108.15/dashboard/docs/images/
https://192.168.108.15/dashboard/docs/images/access-phpmyadmin-remotely/
https://192.168.108.15/dashboard/docs/images/activate-use-xdebug/
https://192.168.108.15/dashboard/docs/images/backup-restore-mysql/
https://192.168.108.15/dashboard/docs/images/configure-vhosts/
https://192.168.108.15/dashboard/docs/images/configure-wildcard-subdomains/
https://192.168.108.15/dashboard/docs/images/send-mail/
https://192.168.108.15/dashboard/docs/images/transfer-files-ftp/
https://192.168.108.15/dashboard/docs/images/troubleshoot-apache/
https://192.168.108.15/dashboard/docs/images/use-different-php-version/
https://192.168.108.15/dashboard/docs/images/use-php-fcgi/
```

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

See Also

http://weakdh.org/

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Risk Factor

Low

CVSS Base Score

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

References

BID	74733
CVE	CVE-2015-4000
XREF	OSVDB:122331

Plugin Information:

Publication date: 2015/05/28, Modification date: 2016/06/16

Ports

tcp/443

```
Vulnerable connection combinations :

  SSL/TLS version  : TLSv1.1
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.1
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_AES_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.1
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_3DES_EDE_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

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

  SSL/TLS version  : TLSv1.1
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_SEED_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
    Warning - This is a known static Oakley Group2 modulus. This may make
    the remote host more vulnerable to the Logjam attack.
  Logjam attack difficulty : Hard (would require nation-state resources)

  SSL/TLS version  : TLSv1.1
  Cipher suite     : TLS1_CK_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
  Diffie-Hellman MODP size (bits) : 1024
```

```
  Warning - This is a known static Oakley Group2 modulus. This may make
  the remote host more vulnerable to the Logjam attack.
Logjam attack difficulty : Hard (would require nation-state resources) [...]
```

94437 - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of 64-bit block ciphers.

Description

The remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites. It is, therefore, affected by a vulnerability, known as SWEET32, due to the use of weak 64-bit block ciphers. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.
Proof-of-concepts have shown that attackers can recover authentication cookies from an HTTPS session in as little as 30 hours.

See Also

https://sweet32.info/

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

Solution

Reconfigure the affected application, if possible, to avoid use of all 64-bit block ciphers.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS Base Score

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

CVSS Temporal Score

2.5 (CVSS2#E:F/RL:ND/RC:ND)

References

BID	92630
BID	92631
CVE	CVE-2016-2183
CVE	CVE-2016-6329
XREF	OSVDB:143387
XREF	OSVDB:143388

Plugin Information:

Publication date: 2016/11/01, Modification date: 2016/12/14

Ports

tcp/443

```
List of 64-bit block cipher suites supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key)

    TLSv1
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      ECDHE-RSA-DES-CBC3-SHA       Kx=ECDH        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

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

```
    TLSv1
      IDEA-CBC-SHA                Kx=RSA          Au=RSA       Enc=IDEA-CBC(128)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

93112 - OpenSSL < 1.1.0 Default Weak 64-bit Block Cipher (SWEET32)

Synopsis

The service running on the remote host uses a weak encryption block cipher by default.

Description

According to its banner, the version of OpenSSL running on the remote host is prior to 1.1.0. It is, therefore, affected by a vulnerability, known as SWEET32, in the 3DES and Blowfish algorithms due to the use of weak 64-bit block ciphers by default. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info/

Solution

Upgrade to OpenSSL version 1.1.0 or later, and ensure all 64-bit block ciphers are disabled. Note that upgrading to OpenSSL 1.1.0 does not completely mitigate this vulnerability; it simply disables the vulnerable 64-bit block ciphers by default.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS Base Score

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

CVSS Temporal Score

2.5 (CVSS2#E:F/RL:ND/RC:ND)

References

BID	92630
CVE	CVE-2016-2183
XREF	OSVDB:143387
XREF	OSVDB:143388

Plugin Information:

Publication date: 2016/08/25, Modification date: 2016/12/07

Ports

tcp/443

```
  Banner           : Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38
  Reported version : 1.0.2h
  Fixed version    : 1.1.0
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/443

```
Port 443/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/11/03

Ports

tcp/443

```
A TLSv1 server answered on this port.
```

tcp/443

```
A web server is running on this port through TLSv1.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/11/03

Ports

tcp/443

```
A TLSv1 server answered on this port.
```

tcp/443

```
A web server is running on this port through TLSv1.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2016/01/11

Ports

tcp/443

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

45410 - SSL Certificate commonName Mismatch

Synopsis

The SSL certificate commonName does not match the host name.

Description

This service presents an SSL certificate for which the 'commonName'
(CN) does not match the host name on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS host name that matches the common name in the certificate.

Risk Factor

None

Plugin Information:

Publication date: 2010/04/03, Modification date: 2012/09/30

Ports

tcp/443

```
The host name known by Nessus is :

  ie10win7

The Common Name in the certificate is :

  localhost
```

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/html/rfc7301

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2015/07/17, Modification date: 2016/02/15

Ports

tcp/443

```
ALPN Supported Protocols:

  http/1.1
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2015/12/30

Ports

tcp/443

```
Subject Name:

Common Name: localhost

Issuer Name:

Common Name: localhost

Serial Number: 00 B5 C7 52 C9 87 81 B5 03

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Nov 10 23:48:47 2009 GMT
Not Valid After: Nov 08 23:48:47 2019 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 C1 25 D3 27 E3 EC AD 0D 83 6A 6D E7 5F 9A 75 10 23 E2 90
            9D A0 63 95 8F 1D 41 9A 58 D5 9C 63 8C 5B 73 86 90 79 CC C3
            D6 A3 89 B8 75 BC 1E 94 7C 7C 6E E3 AD E8 27 5C 0B C6 0C 6A
            F9 0F 32 FE B3 C4 7A 10 23 04 2B 29 28 D4 AA F9 B3 2F 66 10
            F8 A7 C1 CD 60 C4 6B 28 57 E3 67 3B F7 9E CD 48 22 DC 38 EA
            48 13 80 3A 40 97 57 0C 47 35 46 3D 71 62 9A EE 53 9D 63 0E
            67 7A 28 C9 A4 34 FF 19 ED
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 6A F1 F3 49 6C F9 BA 68 5F 6F F3 27 04 C6 B9 0C BD 95 37
           34 BE F7 08 66 9A 9B 03 18 41 BE B9 1D 24 33 55 B6 19 02 1D
           54 71 C9 4F 21 5D 68 75 F3 81 52 41 41 C5 93 C2 1A 7C E2 7B
           C7 4A 24 13 0C 14 9A 4F A7 10 35 0A 6F 6A 0F D3 68 40 FF 48
           44 29 9B 45 6A 0C 5C 29 7C 56 2E B9 F0 4B BD 53 5B 2E 42 B1
           6C AD 97 C1 4B EE D1 1C 68 2D D0 4C 0B FF 3D 1E AA D9 D2 9A
           62 38 DB 90 F9 7D 8C B7 11

Fingerprints :
```

```
SHA-256 Fingerprint: 01 69 73 38 0C 0F 1D F0 0B D9 59 3E D8 D5 EF A3 70 6C D6 DF
                     79 93 F6 14 12 72 B8 05 22 AC DD 23
SHA-1 Fingerprint: B0 23 8C 54 7A 90 5B FA 11 9C 4E 8B AC CA EA CF 36 49 1F F6
MD5 Fingerprint: A0 A4 4C C9 9E 84 B2 6F 9E 63 9F 9E D2 29 DE E0
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.
Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

http://www.openssl.org

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/11/30, Modification date: 2013/10/18

Ports

tcp/443

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/manmaster/apps/ciphers.html

http://www.nessus.org/u?7d537016

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2015/08/27

Ports

tcp/443

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key)
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      ECDHE-RSA-DES-CBC3-SHA       Kx=ECDH        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)
      DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      DHE-RSA-CAMELLIA256-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
```

```
  DHE-RSA-SEED-SHA              Kx=DH        Au=RSA      Enc=SEED-CBC(128)       Mac=SHA1
  ECDHE-RSA-AES128-SHA          Kx=ECDH      Au=RSA      Enc=AES-CBC(128)        Mac=SHA1
  ECDHE-RSA-AES256-SHA          Kx=ECDH      Au=RSA      Enc=AES-CBC(256)        Mac=SHA1
  AES128-SHA                    Kx=RSA       Au=RSA      Enc=AES-CBC(128)        Mac=SHA1
  AES256-SHA                    Kx=RSA       Au=RSA      Enc=AES-CBC(256)        Mac=SHA1
  CAMELLIA128-SHA               Kx=RSA       Au=RSA      Enc=Camellia-CBC(128)   Mac=SHA1
  CAMELLIA256-SHA               Kx=RSA       Au=RSA      Enc=Camellia-CBC(256)   Mac=SHA1
  IDEA-CBC-SHA                  Kx=RSA       Au=RSA      Enc=IDEA-CBC(128)       Mac=SHA1
  SEED-SHA                      Kx=RSA       Au=RSA      Enc=SEED-CBC(128)       Mac=SHA1
  DHE-RSA-AES128-SHA256         Kx=DH        Au=RSA      Enc=AES-CBC(128)        Mac=SHA256

  DHE-RSA-AES256-SHA256         Kx=DH        Au=RSA      Enc=AES-CBC(256)        Mac=SHA256

  ECDHE-RSA-AES128-SHA256       Kx=EC [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

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

http://www.nessus.org/u?cc4a822a

http://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/22, Modification date: 2013/10/22

Ports

tcp/443

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key)

    TLSv1
      EDH-RSA-DES-CBC3-SHA        Kx=DH        Au=RSA      Enc=3DES-CBC(168)       Mac=SHA1
      ECDHE-RSA-DES-CBC3-SHA      Kx=ECDH      Au=RSA      Enc=3DES-CBC(168)       Mac=SHA1
      DES-CBC3-SHA                Kx=RSA       Au=RSA      Enc=3DES-CBC(168)       Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    TLSv1
      DHE-RSA-AES128-SHA          Kx=DH        Au=RSA      Enc=AES-CBC(128)        Mac=SHA1
      DHE-RSA-AES256-SHA          Kx=DH        Au=RSA      Enc=AES-CBC(256)        Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA     Kx=DH        Au=RSA      Enc=Camellia-CBC(128)   Mac=SHA1
      DHE-RSA-CAMELLIA256-SHA     Kx=DH        Au=RSA      Enc=Camellia-CBC(256)   Mac=SHA1
      DHE-RSA-SEED-SHA            Kx=DH        Au=RSA      Enc=SEED-CBC(128)       Mac=SHA1
      ECDHE-RSA-AES128-SHA        Kx=ECDH      Au=RSA      Enc=AES-CBC(128)        Mac=SHA1
      ECDHE-RSA-AES256-SHA        Kx=ECDH      Au=RSA      Enc=AES-CBC(256)        Mac=SHA1
      AES128-SHA                  Kx=RSA       Au=RSA      Enc=AES-CBC(128)        Mac=SHA1
      AES256-SHA                  Kx=RSA       Au=RSA      Enc=AES-CBC(256)        Mac=SHA1
      CAMELLIA128-SHA             Kx=RSA       Au=RSA      Enc=Camellia-CBC(128)   Mac=SHA1
      CAMELLIA256-SHA             Kx=RSA       Au=RSA      Enc=Camellia-CBC(256)   Mac=SHA1
      IDEA-CBC-SHA                Kx=RSA       Au=RSA      Enc=IDEA-CBC(128)       Mac=SHA1
      SEED-SHA                    Kx=RSA       Au=RSA      Enc=SEED-CBC(128)       Mac=SHA1
      DHE-RSA-AES128-SHA256       Kx=DH        Au=RSA      Enc=AES-CBC(128)        Mac=SHA256
```

```
      DHE-RSA-AES256-SHA256        Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA256

      ECDHE-RSA-AES128-SHA256      Kx=ECDHE       Au=RSA      Enc=AES-CBC(1 [...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

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

http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

http://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2012/04/02

Ports

tcp/443

```
Here is the list of SSL PFS ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key)

    TLSv1
      EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
      ECDHE-RSA-DES-CBC3-SHA       Kx=ECDH        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    TLSv1
      DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      DHE-RSA-CAMELLIA128-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(128)    Mac=SHA1
      DHE-RSA-CAMELLIA256-SHA      Kx=DH          Au=RSA      Enc=Camellia-CBC(256)    Mac=SHA1
      DHE-RSA-SEED-SHA             Kx=DH          Au=RSA      Enc=SEED-CBC(128)        Mac=SHA1
      ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA256

      DHE-RSA-AES256-SHA256        Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA256

      ECDHE-RSA-AES128-SHA256      Kx=ECDHE       Au=RSA      Enc=AES-CBC(128)         Mac=SHA256

      ECDHE-RSA-AES256-SHA384      Kx=ECDHE       Au=RSA      Enc=AES-CBC(256)         Mac=SHA384


    TLSv12
      DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256

      DHE-RSA-AES256-SHA384        Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384

      ECDHE-RSA-AES128-SHA256      Kx=ECDHE       Au=RSA      Enc=AES-GCM(128)         Mac=SHA256

      ECDHE-RSA-AES256-SHA384      Kx=ECDHE       Au=RSA      Enc=AES-GCM(256)         Mac=SHA384

The fields above are :
```

```
{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication  [...]
```

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/Predictable-Resource-Location

Solution

n/a

Risk Factor

None

References

XREF	OWASP:OWASP-CM-006

Plugin Information:

Publication date: 2002/06/26, Modification date: 2015/10/13

Ports

tcp/443

```
The following directories were discovered:
/cgi-bin, /error, /icons, /img, /server-info, /server-status, /xampp

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

10662 - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.
It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/05/04, Modification date: 2016/12/08

Ports

tcp/443

```
Webmirror performed 288 queries in 13s (22.0153 queries per second)

The following CGIs have been discovered :


+ CGI : /
  Methods : GET
  Argument :
   Value: util_ldap.c
```

```
Directory index found at /xampp/
Directory index found at /img/
Directory index found at /dashboard/stylesheets/
Directory index found at /dashboard/images/
Directory index found at /dashboard/images/addons/
Directory index found at /dashboard/images/blog/
Directory index found at /dashboard/images/flags/
Directory index found at /dashboard/images/screenshots/
Directory index found at /dashboard/images/stamps/
Directory index found at /dashboard/images/team/
Directory index found at /dashboard/docs/
Directory index found at /dashboard/docs/images/
Directory index found at /dashboard/docs/images/access-phpmyadmin-remotely/
Directory index found at /dashboard/docs/images/activate-use-xdebug/
Directory index found at /dashboard/docs/images/backup-restore-mysql/
Directory index found at /dashboard/docs/images/configure-vhosts/
Directory index found at /dashboard/docs/images/configure-wildcard-subdomains/
Directory index found at /dashboard/docs/images/create-framework-project-zf1/
Directory index found at /dashboard/docs/images/create-framework-project-zf2/
Directory index found at /dashboard/docs/images/deploy-git-app/
Directory index found at /dashboard/docs/images/install-wordpress/
Directory index found at /dashboard/docs/images/reset-mysql-password/
Directory index found at /dashboard/docs/images/send-mail/
Directory index found at /dashboard/docs/images/transfer-files-ftp/
Directory index found at /dashboard/docs/images/troubleshoot-apache/
Directory index found at /dashboard/docs/images/use-different-php-version/
Directory index found at /dashboard/docs/images/use-php-fcgi/
Directory index found at /dashboard/docs/images/use-sqlite/

Extraneous phpinfo() script found at /dashboard/phpinfo.php
```

49704 - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/10/04, Modification date: 2011/08/19

Ports

tcp/443

```
73 external URLs were gathered on this web server :
URL...                                  - Seen on...


http://app01.localhost                  -
http://app02.localhost                  -
http://bitnami.com/stack/xampp?utm_source=bitnami&utm_medium=installer&utm_campaign=XAMPP%2BModule
 -
http://client1/                         -
http://client2/                         -
http://code.google.com/p/gitextensions/ -
http://framework.zend.com/              -
http://framework.zend.com/downloads/latest -
http://framework.zend.com/manual/1.12/en/learning.html -
http://framework.zend.com/manual/2.3/en/user-guide/overview.html -
http://git-extensions-documentation.readthedocs.org/en/latest/getting_started.html -
http://git-scm.com/                     -
http://git-scm.com/book                 -
http://git-scm.com/download/win         -
http://localhost                        -
http://localhost/Slim                   -
http://localhost/example.php            -
```

```
http://localhost/example/phpmailer.php  -
http://localhost/myapp                  -
http://localhost/myapp/                 -
http://localhost/phpMyAdmin             -
http://localhost/sendmail.php           -
http://localhost/sqlite.php             -
http://localhost/wordpress              -
http://localhost/wordpress/wp-login.php -
http://localhost/xampp/phpinfo.php      -
http://myhost                           -
http://phpmailer.worxware.com/          -
http://sourceforge.net/projects/wincachegrind/ -
http://sqlite.org/docs/                 -
http://support.microsoft.com/kb/841290  -
http://wordpress.localhost              -
http://www.apachelounge.com/download/   -
http://www.fastly.com/                  -
http://www.joomla.org/                  -
http://www.kaspersky.com/virusscanner   -
http://www.php.net/                     -
http://www.phpmyadmin.net/              -
http://www.slimframework.com/           -
http://www.sqlite.org/datatype3.html    -
http://www.zend.com/                    -
http://xdebug.org/        [...]
```

50344 - Missing or Permissive Content-Security-Policy HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) response header or does not set one at all.
The CSP header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a properly configured Content-Security-Policy header for all requested resources.

Risk Factor

None

Plugin Information:

Publication date: 2010/10/26, Modification date: 2016/04/14

Ports

tcp/443

```
The following pages do not set a Content-Security-Policy response header or set a permissive
 policy:

  - https://192.168.108.15/applications.html
  - https://192.168.108.15/dashboard/
  - https://192.168.108.15/dashboard/docs/
  - https://192.168.108.15/dashboard/docs/access-phpmyadmin-remotely.html
  - https://192.168.108.15/dashboard/docs/activate-use-xdebug.html
  - https://192.168.108.15/dashboard/docs/backup-restore-mysql.html
  - https://192.168.108.15/dashboard/docs/change-mysql-temp-dir.html
  - https://192.168.108.15/dashboard/docs/configure-vhosts.html
  - https://192.168.108.15/dashboard/docs/configure-wildcard-subdomains.html
  - https://192.168.108.15/dashboard/docs/create-framework-project-zf1.html
  - https://192.168.108.15/dashboard/docs/create-framework-project-zf2.html
  - https://192.168.108.15/dashboard/docs/deploy-git-app.html
  - https://192.168.108.15/dashboard/docs/images/
  - https://192.168.108.15/dashboard/docs/images/access-phpmyadmin-remotely/
  - https://192.168.108.15/dashboard/docs/images/activate-use-xdebug/
```

```
- https://192.168.108.15/dashboard/docs/images/backup-restore-mysql/
- https://192.168.108.15/dashboard/docs/images/configure-vhosts/
- https://192.168.108.15/dashboard/docs/images/configure-wildcard-subdomains/
- https://192.168.108.15/dashboard/docs/images/create-framework-project-zf1/
- https://192.168.108.15/dashboard/docs/images/create-framework-project-zf2/
- https://192.168.108.15/dashboard/docs/images/deploy-git-app/
- https://192.168.108.15/dashboard/docs/images/install-wordpress/
- https://192.168.108.15/dashboard/docs/images/reset-mysql-password/
- https://192.168.108.15/dashboard/docs/images/send-mail/
- https://192.168.108.15/dashboard/docs/images/transfer-files-ftp/
- https://192.168.108.15/dashboard/docs/images/troubleshoot-apache/
- https://192.168.108.15/dashboard/docs/images/use-different-php-version/
- https://192.168.108.15/dashboard/docs/images/use-php-fcgi/
- https://192.168.108.15/dashboard/docs/images/use-sqlite/
- https:/ [...]
```

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.
The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

http://en.wikipedia.org/wiki/Clickjacking

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information:

Publication date: 2010/10/26, Modification date: 2016/04/14

Ports

tcp/443

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - https://192.168.108.15/applications.html
  - https://192.168.108.15/dashboard/
  - https://192.168.108.15/dashboard/docs/
  - https://192.168.108.15/dashboard/docs/access-phpmyadmin-remotely.html
  - https://192.168.108.15/dashboard/docs/activate-use-xdebug.html
  - https://192.168.108.15/dashboard/docs/backup-restore-mysql.html
  - https://192.168.108.15/dashboard/docs/change-mysql-temp-dir.html
  - https://192.168.108.15/dashboard/docs/configure-vhosts.html
  - https://192.168.108.15/dashboard/docs/configure-wildcard-subdomains.html
  - https://192.168.108.15/dashboard/docs/create-framework-project-zf1.html
  - https://192.168.108.15/dashboard/docs/create-framework-project-zf2.html
  - https://192.168.108.15/dashboard/docs/deploy-git-app.html
  - https://192.168.108.15/dashboard/docs/images/
  - https://192.168.108.15/dashboard/docs/images/access-phpmyadmin-remotely/
  - https://192.168.108.15/dashboard/docs/images/activate-use-xdebug/
  - https://192.168.108.15/dashboard/docs/images/backup-restore-mysql/
  - https://192.168.108.15/dashboard/docs/images/configure-vhosts/
  - https://192.168.108.15/dashboard/docs/images/configure-wildcard-subdomains/
  - https://192.168.108.15/dashboard/docs/images/create-framework-project-zf1/
  - https://192.168.108.15/dashboard/docs/images/create-framework-project-zf2/
  - https://192.168.108.15/dashboard/docs/images/deploy-git-app/
  - https://192.168.108.15/dashboard/docs/images/install-wordpress/
  - https://192.168.108.15/dashboard/docs/images/reset-mysql-password/
  - https://192.168.108.15/dashboard/docs/images/send-mail/
  - https://192.168.108.15/dashboard/docs/images/transfer-files-ftp/
  - https://192.168.108.15/dashboard/docs/images/troubleshoot-apache/
```

```
- https://192.168.108.15/dashboard/docs/images/use-different-php-version/
- https://192.168.108.15/dashboard/docs/images/use-php-fcgi/
- https://192.168.108.15/dashboard/docs/images/use-sqlite/
- https://192.168 [...]
```

91815 - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/06/24, Modification date: 2016/06/24

Ports

tcp/443

```
The following sitemap was created from crawling linkable content on the target host :

  - https://192.168.108.15/applications.html
  - https://192.168.108.15/bitnami.css
  - https://192.168.108.15/dashboard/
  - https://192.168.108.15/dashboard/docs/
  - https://192.168.108.15/dashboard/docs/access-phpmyadmin-remotely.html
  - https://192.168.108.15/dashboard/docs/access-phpmyadmin-remotely.pdf
  - https://192.168.108.15/dashboard/docs/activate-use-xdebug.html
  - https://192.168.108.15/dashboard/docs/activate-use-xdebug.pdf
  - https://192.168.108.15/dashboard/docs/activate-use-xdebug.pdfmarks
  - https://192.168.108.15/dashboard/docs/backup-restore-mysql.html
  - https://192.168.108.15/dashboard/docs/backup-restore-mysql.pdf
  - https://192.168.108.15/dashboard/docs/backup-restore-mysql.pdfmarks
  - https://192.168.108.15/dashboard/docs/change-mysql-temp-dir.html
  - https://192.168.108.15/dashboard/docs/change-mysql-temp-dir.pdf
  - https://192.168.108.15/dashboard/docs/change-mysql-temp-dir.pdfmarks
  - https://192.168.108.15/dashboard/docs/configure-vhosts.html
  - https://192.168.108.15/dashboard/docs/configure-vhosts.pdf
  - https://192.168.108.15/dashboard/docs/configure-vhosts.pdfmarks
  - https://192.168.108.15/dashboard/docs/configure-wildcard-subdomains.html
  - https://192.168.108.15/dashboard/docs/configure-wildcard-subdomains.pdf
  - https://192.168.108.15/dashboard/docs/configure-wildcard-subdomains.pdfmarks
  - https://192.168.108.15/dashboard/docs/create-framework-project-zf1.html
  - https://192.168.108.15/dashboard/docs/create-framework-project-zf1.pdf
  - https://192.168.108.15/dashboard/docs/create-framework-project-zf1.pdfmarks
  - https://192.168.108.15/dashboard/docs/create-framework-project-zf2.html
  - https://192.168.108.15/dashboard/docs/create-framework-project-zf2.pdf
  - https://192.168.108.15/dashboard/docs/create-framework-project-zf2.pdfmarks
  - https://192.168.108.15/dashboard/docs/deploy-git-app.html
  - https://192.168.108.15/dashboard/docs/deploy-git-app.pdf
  - https://19 [...]
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2016/02/19

Ports

tcp/443

```
The remote web server type is :

Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.
```

57323 - OpenSSL Version Detection

Synopsis

Nessus was able to detect the OpenSSL version.

Description

Nessus was able to extract the OpenSSL version from the web server's banner. Note that security patches in many cases are backported and the displayed version number does not show the patch level. Using it to identify vulnerable software is likely to lead to false detections.

See Also

http://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/16, Modification date: 2016/11/18

Ports

tcp/443

```
Source              : Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38
Reported version    : 1.0.2h
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/12/10, Modification date: 2013/05/09

Ports

tcp/443

```
Based on the response to an OPTIONS request :
```

```
  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /dashboard
    /dashboard/docs
    /dashboard/docs/images
    /dashboard/docs/images/access-phpmyadmin-remotely
    /dashboard/docs/images/activate-use-xdebug
    /dashboard/docs/images/backup-restore-mysql
    /dashboard/docs/images/configure-vhosts
    /dashboard/docs/images/configure-wildcard-subdomains
    /dashboard/docs/images/create-framework-project-zf1
    /dashboard/docs/images/create-framework-project-zf2
    /dashboard/docs/images/deploy-git-app
    /dashboard/docs/images/install-wordpress
    /dashboard/docs/images/reset-mysql-password
    /dashboard/docs/images/send-mail
    /dashboard/docs/images/transfer-files-ftp
    /dashboard/docs/images/troubleshoot-apache
    /error
    /icons
    /img
    /server-info
    /server-status
    /xampp


Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT COPY DEBUG DELETE GET HEAD INDEX
    LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS
    ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /cgi-bin

  - HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

    /
    /dashboard
    /dashboard/docs
    /dashboard/docs/images
    /dashboard/docs/images/access-phpmyadmin-remotely
    /dashboard/docs/images/activate-use-xdebug
    /dashboard/docs/images/backup-restore-mysql
    /dashboard/docs/images/configure-vhosts
    /dashboard/docs/images/configure-wildcard-subdomains
    /dashboard/docs/images/create-framework-project-zf1
    /dashboard/docs/images/create-framework-project-zf2
    /dashboard/docs/images/deploy-git-app
    /dashboard/docs/images/install-wordpress
    /dashboard/docs/images/reset-mysql-password
    /dashboard/docs/images/send-mail
    /dashboard/docs/images/transfer-files-ft [...]
```

48243 - PHP Version

Synopsis

It is possible to obtain the version number of the remote PHP install.

Description

This plugin attempts to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/08/04, Modification date: 2014/10/31

Ports

tcp/443

```
Nessus was able to identify the following PHP version information :

  Version : 5.5.38
  Source  : Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information:

Publication date: 2015/07/02, Modification date: 2015/07/02

Ports

tcp/443

```
  The remote HTTPS server does not send the HTTP
  "Strict-Transport-Security" header.
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports

tcp/443

```
Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Mon, 19 Dec 2016 07:51:46 GMT
  Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.5.38
  X-Powered-By: PHP/5.5.38
  Location: https://192.168.108.15/dashboard/
  Content-Length: 0
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html
```

91634 - HyperText Transfer Protocol (HTTP) Redirect Information

Synopsis

The remote web server redirects requests to the root directory.

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.
This plugin is informational only and does not denote a security problem.

Solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

Risk Factor

None

Plugin Information:

Publication date: 2016/06/16, Modification date: 2016/06/16

Ports

tcp/443

```
Request         : https://192.168.108.15/
HTTP response   : HTTP/1.1 302 Found
Redirect to     : https://192.168.108.15/dashboard/
Redirect type   : 30x redirect

Final page      : https://192.168.108.15/dashboard/
HTTP response   : HTTP/1.1 200 OK
```

33817 - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.
The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.
Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/10/26, Modification date: 2014/03/12

Ports

tcp/443

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

injectable parameter                    : S=0          SP=0         AP=0         SC=0
 AC=0
blind SQL injection (4 requests)        : S=0          SP=0         AP=0         SC=0
 AC=0
arbitrary command execution (time based) : S=0          SP=0         AP=0         SC=0
 AC=0
cross-site scripting (comprehensive test): S=0          SP=0         AP=0         SC=0
 AC=0
arbitrary command execution             : S=0          SP=0         AP=0         SC=0
 AC=0
directory traversal (extended test)     : S=0          SP=0         AP=0         SC=0
 AC=0
```

```
local file inclusion                    : S=0          SP=0          AP=0          SC=0
 AC=0
web code injection                      : S=0          SP=0          AP=0          SC=0
 AC=0
SQL injection                           : S=0          SP=0          AP=0          SC=0
 AC=0
format string                           : S=0          SP=0          AP=0          SC=0
 AC=0
directory traversal (write access)      : S=0          SP=0          AP=0          SC=0
 AC=0
unseen parameters                       : S=0          SP=0          AP=0          SC=0
 AC=0
XML injection                           : S=0          SP=0          AP=0          SC=0
 AC=0
directory traversal                     : S=0          SP=0          AP=0          SC=0
 AC=0
persistent XSS                          : S=0          SP=0          AP=0          SC=0
 AC=0
SSI injection                           : S=0          SP=0          AP=0          SC=0
 AC=0
SQL injection (2nd order)               : S=0          SP=0          AP=0          SC=0
 AC=0
blind SQL injection                   [...]
```

11419 - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

None

Plugin Information:

Publication date: 2003/03/19, Modification date: 2013/08/13

Ports

tcp/443

```
The following office-related files are available on the remote server :

  - Adobe Acrobat files (.pdf) :
    /dashboard/docs/use-sqlite.pdf
    /dashboard/docs/install-wordpress.pdf
    /dashboard/docs/increase-php-file-upload-limit.pdf
    /dashboard/docs/deploy-git-app.pdf
    /dashboard/docs/create-framework-project-zf2.pdf
    /dashboard/docs/create-framework-project-zf1.pdf
    /dashboard/docs/configure-wildcard-subdomains.pdf
    /dashboard/docs/access-phpmyadmin-remotely.pdf
    /dashboard/docs/activate-use-xdebug.pdf
    /dashboard/docs/backup-restore-mysql.pdf
    /dashboard/docs/change-mysql-temp-dir.pdf
    /dashboard/docs/configure-vhosts.pdf
    /dashboard/docs/reset-mysql-password.pdf
    /dashboard/docs/send-mail.pdf
    /dashboard/docs/transfer-files-ftp.pdf
    /dashboard/docs/troubleshoot-apache.pdf
    /dashboard/docs/use-different-php-version.pdf
    /dashboard/docs/use-php-fcgi.pdf
```

40406 - CGI Generic Tests HTTP Errors

Synopsis

Nessus encountered errors while running its generic CGI attacks.

Description

Nessus ran into trouble while running its generic CGI tests against the remote web server (for example, connection refused, timeout, etc). When this happens, Nessus aborts the current test and switches to the next CGI script on the same port or to another web server. Thus, test results may be incomplete.

Solution

Rescan with a longer network timeout or less parallelism for example, by changing the following options in the scan policy :
- Network -> Network Receive Timeout (check_read_timeout)
- Options -> Number of hosts in parallel (max_hosts)
- Options -> Number of checks in parallel (max_checks)

Risk Factor

None

Plugin Information:

Publication date: 2009/07/28, Modification date: 2011/09/21

Ports

tcp/443

```
Nessus encountered :

  - 1 error involving SQL injection (on HTTP headers) checks :
   . reading the status line: errno=2 (connection reset by peer)
```

445/tcp

57608 - SMB Signing Disabled

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

https://support.microsoft.com/en-us/kb/887429

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

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)

Plugin Information:

Publication date: 2012/01/19, Modification date: 2016/12/09

Ports

tcp/445

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/445

```
A CIFS server is running on this port.
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/445

```
The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\IE10WIN7

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\IE10WIN7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0767a036-0d22-48aa-ba69-b619480f38cb, version 1.0
Description : Unknown RPC service
Annotation : PcaSvc
Type : Remote RPC service
Named pipe : \pipe\trkwks
Netbios name : \\IE10WIN7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
```

```
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\IE10WIN7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\IE10WIN7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Remote RPC service
Named pipe : \PIPE\W32TIME_ALT
Netbios name : \\IE10WIN7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Remote RPC service
Named pipe : \PIPE\DAV RPC SERVICE
Netbios name : \\IE10WIN7

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\IE10W [...]
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It is possible to obtain information about the remote operating system.

Description

It is possible to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. This script requires SMB1 enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/10/17, Modification date: 2016/01/13

Ports

tcp/445

```
The remote Operating System is : Windows 7 Enterprise 7601 Service Pack 1
The remote native lan manager is : Windows 7 Enterprise 6.1
The remote SMB Domain Name is : IE10WIN7
```

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :
- NULL session
- Guest account
- Supplied credentials

See Also

http://support.microsoft.com/kb/143474

http://support.microsoft.com/kb/246261

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2016/03/11

Ports

tcp/445

```
- NULL sessions are enabled on the remote host.
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/445

```
Port 445/tcp was found to be open
```

26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.
If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access'
service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/10/04, Modification date: 2011/03/27

Ports

tcp/445

```
Could not connect to the registry because:
Could not connect to \winreg
```

554/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/554

```
Port 554/tcp was found to be open
```

1900/udp

35711 - Universal Plug and Play (UPnP) Protocol Detection

Synopsis

The remote device supports UPnP.

Description

The remote device answered an SSDP M-SEARCH request. Therefore, it supports 'Universal Plug and Play' (UPnP). This protocol provides automatic configuration and device discovery. It is primarily intended for home networks. An attacker could potentially leverage this to discover your network architecture.

See Also

http://en.wikipedia.org/wiki/Universal_Plug_and_Play

http://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol

http://quimby.gnus.org/internet-drafts/draft-cai-ssdp-v1-03.txt

Solution

Filter access to this port if desired.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2016/10/13

Ports

udp/1900

```
The device responded to an SSDP M-SEARCH request with the following locations :

    http://192.168.108.15:2869/upnphost/udhisapi.dll?content=uuid:9fabbe94-64d1-4621-
a9dc-92efb8006511

And advertises these unique service names :

    uuid:9fabbe94-64d1-4621-
a9dc-92efb8006511::urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1
    uuid:9fabbe94-64d1-4621-a9dc-92efb8006511::upnp:rootdevice
    uuid:9fabbe94-64d1-4621-a9dc-92efb8006511::urn:schemas-upnp-org:service:ConnectionManager:1
    uuid:9fabbe94-64d1-4621-a9dc-92efb8006511::urn:schemas-upnp-org:device:MediaServer:1
    uuid:9fabbe94-64d1-4621-a9dc-92efb8006511::urn:schemas-upnp-org:service:ContentDirectory:1
```

2103/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/2103

```
The following DCERPC services are available on TCP port 2103 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V1
Type : Remote RPC service
TCP Port : 2103
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V2
Type : Remote RPC service
TCP Port : 2103
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QM2QM V1
Type : Remote RPC service
TCP Port : 2103
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0
Description : Unknown RPC service
Annotation : Message Queuing - RemoteRead V1
Type : Remote RPC service
TCP Port : 2103
IP : 192.168.108.15
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/2103

```
Port 2103/tcp was found to be open
```

2105/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/2105

```
The following DCERPC services are available on TCP port 2105 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V1
Type : Remote RPC service
TCP Port : 2105
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V2
Type : Remote RPC service
TCP Port : 2105
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QM2QM V1
Type : Remote RPC service
TCP Port : 2105
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0
Description : Unknown RPC service
Annotation : Message Queuing - RemoteRead V1
Type : Remote RPC service
TCP Port : 2105
IP : 192.168.108.15
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/2105

```
Port 2105/tcp was found to be open
```

2107/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/2107

```
The following DCERPC services are available on TCP port 2107 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V1
Type : Remote RPC service
TCP Port : 2107
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V2
Type : Remote RPC service
TCP Port : 2107
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QM2QM V1
Type : Remote RPC service
```

```
TCP Port : 2107
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0
Description : Unknown RPC service
Annotation : Message Queuing - RemoteRead V1
Type : Remote RPC service
TCP Port : 2107
IP : 192.168.108.15
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/2107

```
Port 2107/tcp was found to be open
```

2224/tcp

85582 - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.
X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.
Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.
Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

http://www.nessus.org/u?399b1f56

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

http://en.wikipedia.org/wiki/Clickjacking

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.
This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Risk Factor

Medium

CVSS Base Score

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

References

XREF	CWE:693

Plugin Information:

Publication date: 2015/08/22, Modification date: 2016/11/18

Ports

tcp/2224

```
The following pages do not use a clickjacking mitigation response header and contain a clickable
 event :

  - http://192.168.108.15:2224/mlss
```

26194 - Web Server Transmits Cleartext Credentials

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.
An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS Base Score

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

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information:

Publication date: 2007/09/28, Modification date: 2016/11/29

Ports

tcp/2224

```
Page : /mlss
Destination Page: /mlss/ManageSubscription
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/2224

```
Port 2224/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/11/03

Ports

tcp/2224

```
A web server is running on this port.
```

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/Predictable-Resource-Location

Solution

n/a

Risk Factor

None

References

XREF	OWASP:OWASP-CM-006

Plugin Information:

Publication date: 2002/06/26, Modification date: 2015/10/13

Ports

tcp/2224

```
The following directories were discovered:
/Mail, /mail
```

```
While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

10662 - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.
It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/05/04, Modification date: 2016/12/08

Ports

tcp/2224

```
Webmirror performed 8 queries in 1s (8.000 queries per second)

The following CGIs have been discovered :


+ CGI : /mlss/SubscribeToList
  Methods : POST
  Argument : SubProceed
   Value: Proceed...


+ CGI : /mlss/ManageSubscription
  Methods : GET
  Argument : MSubEmailAddress
  Argument : MSubPwd
  Argument : MSubscription
   Value: Subscription...


+ CGI : /mlss/ForgotPassword
  Methods : POST
  Argument : EmailAddress
  Argument : ForgotPassword
   Value: Mail password...


+ CGI : /mlss/MassChange
  Methods : POST
  Argument : EmailAddress
  Argument : ListStatus
   Value: StatusUnsubscribe
  Argument : MassChangeStatus
   Value: Set Status...
```

49704 - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/10/04, Modification date: 2011/08/19

Ports

tcp/2224

```
1 external URL was gathered on this web server :
URL...                                  - Seen on...


http://localhost:2224/mlss              - /mlss/SubscribeToList
```

50344 - Missing or Permissive Content-Security-Policy HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) response header or does not set one at all.
The CSP header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a properly configured Content-Security-Policy header for all requested resources.

Risk Factor

None

Plugin Information:

Publication date: 2010/10/26, Modification date: 2016/04/14

Ports

tcp/2224

```
The following pages do not set a Content-Security-Policy response header or set a permissive
 policy:

  - http://192.168.108.15:2224/
  - http://192.168.108.15:2224/mlss
  - http://192.168.108.15:2224/mlss/ForgotPassword
  - http://192.168.108.15:2224/mlss/ManageSubscription
  - http://192.168.108.15:2224/mlss/MassChange
  - http://192.168.108.15:2224/mlss/SubscribeToList
```

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.
The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

http://en.wikipedia.org/wiki/Clickjacking

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information:

Publication date: 2010/10/26, Modification date: 2016/04/14

Ports

tcp/2224

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://192.168.108.15:2224/
  - http://192.168.108.15:2224/mlss
  - http://192.168.108.15:2224/mlss/ForgotPassword
  - http://192.168.108.15:2224/mlss/ManageSubscription
  - http://192.168.108.15:2224/mlss/MassChange
  - http://192.168.108.15:2224/mlss/SubscribeToList
```

91815 - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/06/24, Modification date: 2016/06/24

Ports

tcp/2224

```
The following sitemap was created from crawling linkable content on the target host :

  - http://192.168.108.15:2224/
  - http://192.168.108.15:2224/Mail
  - http://192.168.108.15:2224/mail
  - http://192.168.108.15:2224/mlss
  - http://192.168.108.15:2224/mlss/ForgotPassword
  - http://192.168.108.15:2224/mlss/ManageSubscription
  - http://192.168.108.15:2224/mlss/MassChange
  - http://192.168.108.15:2224/mlss/SubscribeToList

Attached is a copy of the sitemap file.
```

42057 - Web Server Allows Password Auto-Completion

Synopsis

The 'autocomplete' attribute is not disabled on password fields.

Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.
While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

None

Plugin Information:

Publication date: 2009/10/07, Modification date: 2016/06/16

Ports

tcp/2224

```
Page : /mlss
Destination Page: /mlss/ManageSubscription
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports

tcp/2224

```
Protocol version : HTTP/1.0
SSL : no
Keep-Alive : no
Headers :

  Content-type: text/html
  Content-Length: 2841
```

33817 - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.
The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.
Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/10/26, Modification date: 2014/03/12

Ports

tcp/2224

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]
```

```
cross-site scripting (comprehensive test): S=36         SP=64        AP=64        SC=68
 AC=68
directory traversal (write access)       : S=18         SP=32        AP=32        SC=34
 AC=34
SSI injection                            : S=27         SP=48        AP=48        SC=51
 AC=51
arbitrary command execution (time based) : S=54         SP=96        AP=96        SC=102
 AC=102
local file inclusion                     : S=9          SP=16        AP=16        SC=17
 AC=17
format string                            : S=18         SP=32        AP=32        SC=34
 AC=34
blind SQL injection (4 requests)         : S=36         SP=64        AP=64        SC=68
 AC=68
directory traversal (extended test)      : S=459        SP=816       AP=816       SC=867
 AC=867
injectable parameter                     : S=18         SP=32        AP=32        SC=34
 AC=34
unseen parameters                        : S=315        SP=560       AP=560       SC=595
 AC=595
XML injection                            : S=9          SP=16        AP=16        SC=17
 AC=17
persistent XSS                           : S=36         SP=64        AP=64        SC=68
 AC=68
web code injection                       : S=9          SP=16        AP=16        SC=17
 AC=17
SQL injection (2nd order)                : S=9          SP=16        AP=16        SC=17
 AC=17
blind SQL injection                      : S=108        SP=192       AP=192       SC=204
 AC=204
SQL injection                            : S=216        SP=384       AP=384       SC=408
 AC=408
arbitrary command execution              : S=144        SP=256       AP=256       SC=272
 AC=272
directory traversal                    [...]
```

40406 - CGI Generic Tests HTTP Errors

Synopsis

Nessus encountered errors while running its generic CGI attacks.

Description

Nessus ran into trouble while running its generic CGI tests against the remote web server (for example, connection refused, timeout, etc). When this happens, Nessus aborts the current test and switches to the next CGI script on the same port or to another web server. Thus, test results may be incomplete.

Solution

Rescan with a longer network timeout or less parallelism for example, by changing the following options in the scan policy :
- Network -> Network Receive Timeout (check_read_timeout)
- Options -> Number of hosts in parallel (max_hosts)
- Options -> Number of checks in parallel (max_checks)

Risk Factor

None

Plugin Information:

Publication date: 2009/07/28, Modification date: 2011/09/21

Ports

tcp/2224

```
Nessus encountered :

  - 2 errors involving SQL injection (on HTTP headers) checks :
   . connecting to server: errno=6 (connection refused)
  - 4 errors involving XSS (on HTTP headers) checks :
   . connecting to server: errno=6 (connection refused)
   . reading the HTTP status line: errno=2 (connection reset by peer)
  - 4 errors involving persistent XSS checks :

This web server appears to be unresponsive now.
```

2869/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/2869

```
Port 2869/tcp was found to be open
```

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'
request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/11/18, Modification date: 2016/05/26

Ports

tcp/2869

```
A web server seems to be running on this port.
```

35712 - Web Server UPnP Detection

Synopsis

The remote web server provides UPnP information.

Description

Nessus was able to extract some information about the UPnP-enabled device by querying this web server. Services may also be reachable through SOAP requests.

See Also

http://en.wikipedia.org/wiki/Universal_Plug_and_Play

Solution

Filter incoming traffic to this port if desired.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2016/10/13

Ports
tcp/2869

```
Here is a summary of http://192.168.108.15:2869/upnphost/udhisapi.dll?
content=uuid:9fabbe94-64d1-4621-a9dc-92efb8006511 :

deviceType: urn:schemas-upnp-org:device:MediaServer:1
friendlyName: IE10WIN7: IEUser:
manufacturer: Microsoft Corporation
manufacturerURL: http://www.microsoft.com
modelName: Windows Media Player Sharing
modelName: Windows Media Player Sharing
modelNumber: 12.0
modelURL: http://go.microsoft.com/fwlink/?LinkId=105926
serialNumber: {C1703A18-086D-4CD3-8312-54318CC6449D}
ServiceID: urn:upnp-org:serviceId:ConnectionManager
 serviceType: urn:schemas-upnp-org:service:ConnectionManager:1
 controlURL: /upnphost/udhisapi.dll?control=uuid:9fabbe94-64d1-4621-a9dc-92efb8006511+urn:upnp-
org:serviceId:ConnectionManager
 eventSubURL: /upnphost/udhisapi.dll?event=uuid:9fabbe94-64d1-4621-a9dc-92efb8006511+urn:upnp-
org:serviceId:ConnectionManager
 SCPDURL: /upnphost/udhisapi.dll?content=uuid:d06d7943-fe3e-4e49-b034-1bea0f563a7f
ServiceID: urn:upnp-org:serviceId:ContentDirectory
 serviceType: urn:schemas-upnp-org:service:ContentDirectory:1
 controlURL: /upnphost/udhisapi.dll?control=uuid:9fabbe94-64d1-4621-a9dc-92efb8006511+urn:upnp-
org:serviceId:ContentDirectory
 eventSubURL: /upnphost/udhisapi.dll?event=uuid:9fabbe94-64d1-4621-a9dc-92efb8006511+urn:upnp-
org:serviceId:ContentDirectory
 SCPDURL: /upnphost/udhisapi.dll?content=uuid:ccbba2a3-0ce1-4acf-b58f-f768acfd7f5c
ServiceID: urn:microsoft.com:serviceId:X_MS_MediaReceiverRegistrar
 serviceType: urn:microsoft.com:service:X_MS_MediaReceiverRegistrar:1
 controlURL: /upnphost/udhisapi.dll?control=uuid:9fabbe94-64d1-4621-
a9dc-92efb8006511+urn:microsoft.com:serviceId:X_MS_MediaReceiverRegistrar
 eventSubURL: /upnphost/udhisapi.dll?event=uuid:9fabbe94-64d1-4621-
a9dc-92efb8006511+urn:microsoft.com:serviceId:X_MS_MediaReceiverRegistrar
 SCPDURL: /upnphost/udhisapi.dll?content=uuid:9023bbc3-7aac-4923-b6e0-a5fb66768609
```

3306/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports
tcp/3306

```
Port 3306/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2016/11/03

Ports

tcp/3306

```
A MariaDB server is running on this port.
```

3389/tcp

51192 - 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 unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

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)

Plugin Information:

Publication date: 2010/12/15, Modification date: 2015/10/21

Ports

tcp/3389

```
The following certificate was at the top of the certificate
chain sent by the remote host, but is signed by an unknown
certificate authority :

|-Subject : CN=IE10Win7
|-Issuer  : CN=IE10Win7
```

35291 - 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 (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.
Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

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)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	OSVDB:45106
XREF	OSVDB:45108
XREF	OSVDB:45127
XREF	CERT:836068
XREF	CWE:310

Plugin Information:

Publication date: 2009/01/05, Modification date: 2016/09/19

Ports

tcp/3389

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

|-Subject             : CN=IE10Win7
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Dec 13 07:00:59 2016 GMT
|-Valid To            : Jun 14 07:00:59 2017 GMT
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

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)

Plugin Information:

Publication date: 2012/01/17, Modification date: 2016/12/14

Ports

tcp/3389

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=IE10Win7
```

42873 - 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)

Plugin Information:

Publication date: 2009/11/23, Modification date: 2015/10/21

Ports

tcp/3389

```
Here is the list of medium strength SSL ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key)

    TLSv1
      DES-CBC3-SHA                Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

58453 - 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

http://www.nessus.org/u?e2628096

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)

Plugin Information:

Publication date: 2012/03/23, Modification date: 2016/10/20

Ports

tcp/3389

```
Nessus was able to negotiate non-NLA (Network Level Authentication) security.
```

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)

Plugin Information:

Publication date: 2012/01/25, Modification date: 2016/10/20

Ports

tcp/3389

```
The terminal services encryption level is set to :

2. Medium
```

18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

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://www.nessus.org/u?e2628096

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)

References

BID	13818
CVE	CVE-2005-1794
XREF	OSVDB:17131

Plugin Information:

Publication date: 2005/06/01, Modification date: 2016/11/23

Ports

tcp/3389

94437 - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of 64-bit block ciphers.

Description

The remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites. It is, therefore, affected by a vulnerability, known as SWEET32, due to the use of weak 64-bit block ciphers. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.
Proof-of-concepts have shown that attackers can recover authentication cookies from an HTTPS session in as little as 30 hours.

See Also

https://sweet32.info/

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

Solution

Reconfigure the affected application, if possible, to avoid use of all 64-bit block ciphers.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS Base Score

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

CVSS Temporal Score

2.5 (CVSS2#E:F/RL:ND/RC:ND)

References

BID	92630
BID	92631
CVE	CVE-2016-2183
CVE	CVE-2016-6329
XREF	OSVDB:143387
XREF	OSVDB:143388

Plugin Information:

Publication date: 2016/11/01, Modification date: 2016/12/14

Ports

tcp/3389

```
List of 64-bit block cipher suites supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key)

    TLSv1
      DES-CBC3-SHA                Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

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://www.nessus.org/u?217a3666

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.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

2.2 (CVSS2#E:F/RL:TF/RC:ND)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808
XREF	OSVDB:91162
XREF	OSVDB:117855

Plugin Information:

Publication date: 2013/04/05, Modification date: 2016/12/14

Ports

tcp/3389

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    TLSv1
      RC4-MD5                     Kx=RSA         Au=RSA       Enc=RC4(128)             Mac=MD5
      RC4-SHA                     Kx=RSA         Au=RSA       Enc=RC4(128)             Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

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)

Plugin Information:

Publication date: 2008/02/11, Modification date: 2016/10/20

Ports

tcp/3389

```
The terminal services encryption level is set to :

2. Medium (Client Compatible)
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2016/10/18

Ports

tcp/3389

```
Port 3389/tcp was found to be open
```

10940 - Windows Terminal Services Enabled

Synopsis

The remote Windows host has Terminal Services enabled.

Description

Terminal Services allows a Windows user to remotely obtain a graphical login (and therefore act as a local user on the remote host).
If an attacker gains a valid login and password, this service could be used to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.
Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.

Solution

Disable Terminal Services if you do not use it, and do not allow this service to run across the Internet.

Risk Factor

None

Plugin Information:

Publication date: 2002/04/20, Modification date: 2014/06/06

Ports

tcp/3389

66173 - RDP Screenshot

Synopsis

It is possible to take a screenshot of the remote login screen.

Description

This script attempts to connect to the remote host via RDP (Remote Desktop Protocol) and attempts to take a screenshot of the login screen.
While this is not a vulnerability by itself, some versions of Windows display the names of the users who can connect and which ones are connected already.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/04/22, Modification date: 2016/10/20

Ports

tcp/3389

It was possible to gather the following screenshot of the remote login screen.

64814 - Terminal Services Use SSL/TLS

Synopsis

The remote Terminal Services use SSL/TLS.

Description

The remote Terminal Services is configured to use SSL/TLS.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/02/22, Modification date: 2016/01/19

Ports

tcp/3389

```
Subject Name:

Common Name: IE10Win7

Issuer Name:

Common Name: IE10Win7

Serial Number: 45 54 78 62 2A 49 1B B0 43 8B 11 D9 13 92 E0 B0

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Dec 13 07:00:59 2016 GMT
Not Valid After: Jun 14 07:00:59 2017 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 92 9F DF B2 38 7B B1 A6 FF C8 95 39 60 74 73 D9 01 69 AE
            BD C0 89 90 DB 88 2B 33 C9 1F 5D 79 62 6F 2A 5C E8 C1 25 DF
            75 FE 45 CE F6 B2 8C B6 E6 3F 1D 5B D8 EF F1 8F 23 3A 76 6A
            DA 28 2E B8 F7 25 CE 11 10 ED 34 22 43 7E B8 5C 6D 63 A2 02
            00 E1 39 85 4D 65 C0 1D 5B 80 52 E6 60 D7 7E 0B 5D 1D 6E 4E
            10 7B 66 C9 8D AF 4C 66 BC 54 16 9F ED 5C 83 3B 00 B9 A4 E7
            DE 9F 68 06 19 85 A4 74 91 26 C9 D3 A9 37 B6 3C 19 46 09 BC
            7E 52 6A F1 67 B8 C2 C5 19 06 4C 00 A2 0D 04 2A 5E D5 C1 04
            2A 16 62 5D 27 20 B0 CE A4 73 BA 16 FB 81 00 95 3D B2 70 2A
            EE 72 83 E6 A5 4F E8 9B 8F BE 9C 7F FA 39 B0 B4 5D 86 56 3E
            6C 6A 44 EC CE A5 F2 6C 80 73 A6 CB AC CD FB 7B 2D 78 91 8E
            A0 AA D1 3B 9B E4 2E AD 18 59 7A E9 C6 62 3A AF 7F 7A 47 85
            B0 DF 63 62 10 B8 F4 2F BE 16 A0 E2 3C 61 CC 62 49
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 41 44 64 24 CE 98 DA A6 8A 9A 1A 95 6C 80 9C 9B F6 57 D4
           70 8C B2 4A F9 BD B9 A9 8E 29 0D BB EF BD 03 38 47 DE EE 73
           B8 BD 57 05 54 CF 21 D4 64 F8 18 88 3E AB 39 2F 20 C6 08 24
           64 07 41 BD F6 8E 88 0A F1 76 1E C4 7D 7C 49 0B B7 F5 FE 9C
           A0 86 A7 D1 7B 85 62 5D A5 77 05 21 F5 A2 9D EC 76 C6 8C 5D
           9A 12 21 4A CB 8B 68 D6 2A 44 BA 78 06 EF CF E7 55 18 5F 42
           79 D5 DF 7E 50 B2 4C FC 87 1A DC B9 2D 3A 4A 63 5F 6B BB E0
           15 EE BC 48 D8 F2 C8 23 E3 8A 5A 8D C1 2F 80 62 78 31 2F 0A
           C1 59 67 71 C6 52 50 6E 1B 03 E7 30 9F 0C 92 FF 6B 28 BD FC
           EA 11 7F D5 34 5A 16 42 60 F5 05 F [...]
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2016/01/11

Ports

tcp/3389

```
This port supports TLSv1.0.
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2015/12/30

Ports

tcp/3389

```
Subject Name:

Common Name: IE10Win7

Issuer Name:

Common Name: IE10Win7

Serial Number: 45 54 78 62 2A 49 1B B0 43 8B 11 D9 13 92 E0 B0

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Dec 13 07:00:59 2016 GMT
Not Valid After: Jun 14 07:00:59 2017 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 92 9F DF B2 38 7B B1 A6 FF C8 95 39 60 74 73 D9 01 69 AE
            BD C0 89 90 DB 88 2B 33 C9 1F 5D 79 62 6F 2A 5C E8 C1 25 DF
            75 FE 45 CE F6 B2 8C B6 E6 3F 1D 5B D8 EF F1 8F 23 3A 76 6A
            DA 28 2E B8 F7 25 CE 11 10 ED 34 22 43 7E B8 5C 6D 63 A2 02
            00 E1 39 85 4D 65 C0 1D 5B 80 52 E6 60 D7 7E 0B 5D 1D 6E 4E
            10 7B 66 C9 8D AF 4C 66 BC 54 16 9F ED 5C 83 3B 00 B9 A4 E7
            DE 9F 68 06 19 85 A4 74 91 26 C9 D3 A9 37 B6 3C 19 46 09 BC
            7E 52 6A F1 67 B8 C2 C5 19 06 4C 00 A2 0D 04 2A 5E D5 C1 04
            2A 16 62 5D 27 20 B0 CE A4 73 BA 16 FB 81 00 95 3D B2 70 2A
            EE 72 83 E6 A5 4F E8 9B 8F BE 9C 7F FA 39 B0 B4 5D 86 56 3E
            6C 6A 44 EC CE A5 F2 6C 80 73 A6 CB AC CD FB 7B 2D 78 91 8E
            A0 AA D1 3B 9B E4 2E AD 18 59 7A E9 C6 62 3A AF 7F 7A 47 85
            B0 DF 63 62 10 B8 F4 2F BE 16 A0 E2 3C 61 CC 62 49
Exponent: 01 00 01
```

```
Signature Length: 256 bytes / 2048 bits
Signature: 00 41 44 64 24 CE 98 DA A6 8A 9A 1A 95 6C 80 9C 9B F6 57 D4
           70 8C B2 4A F9 BD B9 A9 8E 29 0D BB EF BD 03 38 47 DE EE 73
           B8 BD 57 05 54 CF 21 D4 64 F8 18 88 3E AB 39 2F 20 C6 08 24
           64 07 41 BD F6 8E 88 0A F1 76 1E C4 7D 7C 49 0B B7 F5 FE 9C
           A0 86 A7 D1 7B 85 62 5D A5 77 05 21 F5 A2 9D EC 76 C6 8C 5D
           9A 12 21 4A CB 8B 68 D6 2A 44 BA 78 06 EF CF E7 55 18 5F 42
           79 D5 DF 7E 50 B2 4C FC 87 1A DC B9 2D 3A 4A 63 5F 6B BB E0
           15 EE BC 48 D8 F2 C8 23 E3 8A 5A 8D C1 2F 80 62 78 31 2F 0A
           C1 59 67 71 C6 52 50 6E 1B 03 E7 30 9F 0C 92 FF 6B 28 BD FC
           EA 11 7F D5 34 5A 16 42 60 F5 05 F [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/manmaster/apps/ciphers.html

http://www.nessus.org/u?7d537016

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2015/08/27

Ports

tcp/3389

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv1
  Medium Strength Ciphers (> 64-bit and < 112-bit key)
      DES-CBC3-SHA                Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)
      ECDHE-RSA-AES128-SHA        Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      ECDHE-RSA-AES256-SHA        Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      AES128-SHA                  Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      AES256-SHA                  Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
      RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

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

http://www.nessus.org/u?cc4a822a

http://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/22, Modification date: 2013/10/22

Ports

tcp/3389

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key)

    TLSv1
      DES-CBC3-SHA                Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

  High Strength Ciphers (>= 112-bit key)

    TLSv1
      ECDHE-RSA-AES128-SHA        Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      ECDHE-RSA-AES256-SHA        Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
      AES128-SHA                  Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      AES256-SHA                  Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

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

http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

http://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2012/04/02

Ports
tcp/3389

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    TLSv1
      ECDHE-RSA-AES128-SHA         Kx=ECDH       Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
      ECDHE-RSA-AES256-SHA         Kx=ECDH       Au=RSA      Enc=AES-CBC(256)         Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/02/07, Modification date: 2013/10/18

Ports
tcp/3389

```
This port supports resuming TLSv1 sessions.
```

5355/udp

53513 - Link-Local Multicast Name Resolution (LLMNR) Detection

Synopsis

The remote device supports LLMNR.

Description

The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions.

See Also

http://www.nessus.org/u?85beb421

http://technet.microsoft.com/en-us/library/bb878128.aspx

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2011/04/21, Modification date: 2012/03/05

Ports
udp/5355

```
According to LLMNR, the name of the remote host is 'IE10Win7'.
```

49152/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49152

```
The following DCERPC services are available on TCP port 49152 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49152
IP : 192.168.108.15
```

49153/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49153

```
The following DCERPC services are available on TCP port 49153 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
```

```
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.108.15
```

49154/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49154

```
The following DCERPC services are available on TCP port 49154 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.108.15
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.108.15

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1.0
Description : Unknown RPC service
Annotation : [...]
```

49155/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49155

```
The following DCERPC services are available on TCP port 49155 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fdb3a030-065f-11d1-bb9b-00a024ea5525, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V1
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76d12b80-3467-11d3-91ff-0090272f9ea3, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QMRT V2
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1088a980-eae5-11d0-8d9b-00a02453c337, version 1.0
Description : Message Queuing Service
Windows process : mqsvc.exe
Annotation : Message Queuing - QM2QM V1
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1a9134dd-7b39-45ba-ad88-44d01ca47f28, version 1.0
Description : Unknown RPC service
Annotation : Message Queuing - RemoteRead V1
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.108.15
```

49156/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49156

```
The following DCERPC services are available on TCP port 49156 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.108.15
```

49157/tcp

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49157

```
The following DCERPC services are available on TCP port 49157 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1.0
Description : Unknown RPC service
Annotation : Remote Fw APIs
Type : Remote RPC service
TCP Port : 49157
IP : 192.168.108.15

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Remote RPC service
TCP Port : 49157
IP : 192.168.108.15
```

49158/tcp

90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Synopsis

The remote Windows host is affected by an elevation of privilege vulnerability.

Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

See Also

https://technet.microsoft.com/library/security/MS16-047

http://badlock.org/

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

5.6 (CVSS2#E:F/RL:OF/RC:ND)

STIG Severity

I

References

BID	86002
CVE	CVE-2016-0128
XREF	OSVDB:136339
XREF	MSFT:MS16-047
XREF	CERT:813296
XREF	IAVA:2016-A-0093

Plugin Information:

Publication date: 2016/04/13, Modification date: 2016/07/19

Ports

tcp/49158

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2014/05/12

Ports

tcp/49158

```
The following DCERPC services are available on TCP port 49158 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49158
IP : 192.168.108.15
```

Remediations

Suggested Remediations

Taking the following actions across 1 hosts would resolve 3% of the vulnerabilities on the network:

Action to take	Vulns	Hosts
FileZilla Server < 0.9.31 Denial of Service: Upgrade to FileZilla Server version 0.9.31 or later.	1	1
OpenSSL 1.0.2 < 1.0.2i Multiple Vulnerabilities (SWEET32): Upgrade to OpenSSL version 1.0.2i or later. Note that the GOST ciphersuites vulnerability (VulnDB 144759) is not yet fixed by the vendor in an official release; however, a patch for the issue has been committed to the OpenSSL github repository.	1	1