



hands-on-basic-network

Report generated by NessusTM

Tue, 19 Jun 2018 12:03:49 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

192.168.17.1.....	4
192.168.17.10.....	32
192.168.17.21.....	56
192.168.17.31.....	234
192.168.17.41.....	309
192.168.17.53.....	372
192.168.17.252.....	673
192.168.17.253.....	736
192.168.17.254.....	775

Remediations

Suggested Remediations.....	829
-----------------------------	-----

Vulnerabilities by Host

192.168.17.1

0

CRITICAL

0

HIGH

0

MEDIUM

0

LOW

22

INFO

Scan Information

Start time: Tue Jun 19 10:40:12 2018

End time: Tue Jun 19 10:47:57 2018

Host Information

IP: 192.168.17.1

OS: Linux Kernel 4.4 on Ubuntu 16.04 (xenial)

Vulnerabilities

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:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

icmp/0

```
The difference between the local and remote clocks is 209 seconds.
```

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:

Published: 2003/12/09, Modified: 2018/04/19

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
Confidence level : 95
Method : SSH
```

```
The remote host is running Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
```

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

n/a

Risk Factor

None

Plugin Information:

Published: 2005/05/15, Modified: 2017/03/13

Plugin Output

tcp/0

```
The Linux distribution detected was :  
- Ubuntu 16.04 (xenial)  
- Ubuntu 16.10 (yakkety)
```

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:

Published: 2005/08/26, Modified: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :  
  
Nessus version : 7.1.1  
Plugin feed version : 201806151820  
Scanner edition used : Nessus  
Scan type : Normal  
Scan policy used : Basic Network Scan  
Scanner IP : 192.168.1.235  
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 : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2018/6/19 10:40 CEST
Scan duration : 442 sec
```

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:

Published: 2007/05/16, Modified: 2011/03/20

Plugin Output

tcp/0

Synopsis

It was 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/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/04/21, Modified: 2017/06/06

Plugin Output

tcp/0

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

```
cpe:/o:canonical:ubuntu_linux:16.04
```

```
Following application CPE's matched on the remote system :
```

```
cpe:/a:openbsd:openssh:7.2
```

```
cpe:/a:apache:http_server:2.4.18
```

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:

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 95
```

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/11/27, Modified: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.235 to 192.168.17.1 :
192.168.1.235
192.168.7.252
192.168.17.1
```

```
Hop Count: 2
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/10/12, Modified: 2017/12/19

Plugin Output

tcp/22

```
SSH version : SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2
SSH supported authentication : publickey,password
SSH banner :
#####
#                Welcome to this server                #
#      All connections are monitored and recorded      #
#      Disconnect IMMEDIATELY if you are not an authorized user!  #
#####
```

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/03/06, Modified: 2017/05/30

Plugin Output

tcp/22

```
The remote SSH daemon supports the following versions of the
SSH protocol :
```

- 1.99
- 2.0

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/22

```
Port 22/tcp was found to be open
```


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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/22

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

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22

```
Give Nessus credentials to perform local checks.
```

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22

```
Nessus negotiated the following encryption algorithm with the server :
```

```
The server supports the following options for kex_algorithms :
```

```
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha1
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
```

```
The server supports the following options for server_host_key_algorithms :
```

```
ecdsa-sha2-nistp256
rsa-sha2-256
rsa-sha2-512
ssh-ed25519
ssh-rsa
```

```
The server supports the following options for encryption_algorithms_client_to_server :
```

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

```
The server supports the following options for encryption_algorithms_server_to_client :
```

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

The server supports the following options for `mac_algorithms_client_to_server` :

```
hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
```

The server supports the following options for `mac_algorithms_server_to_client` :

```
hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
```

The server supports the following options for `compression_algorithms_client_to_server` :

```
none
```

The server supports the following options for `compression_algorithms_server_to_client` :

```
none
```

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:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/80

```
The remote web server type is :  
Apache/2.4.18 (Ubuntu)
```

Synopsis

A transparent or reverse HTTP proxy is running on this port.

Description

This web server is reachable through a reverse HTTP proxy.

Solution

n/a

Risk Factor

None

References

CVE	CVE-2004-2320
CVE	CVE-2005-3398
CVE	CVE-2005-3498
CVE	CVE-2007-3008
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:35511
XREF	OSVDB:50485
XREF	CWE:200
XREF	CWE:79

Plugin Information:

Published: 2002/07/02, Modified: 2018/05/21

Plugin Output

tcp/80

```
There might be a caching proxy on the way to this web server:
MISS from localhost
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/80

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

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/80

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


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:

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/80

```
Response Code : HTTP/1.1 200 OK
```

```
Protocol version : HTTP/1.1
```

```
SSL : no
```

```
Keep-Alive : no
```

```
Options allowed : (Not implemented)
```

```
Headers :
```

```
Date: Tue, 19 Jun 2018 08:43:03 GMT
```

```
Server: Apache/2.4.18 (Ubuntu)
```

```
Last-Modified: Tue, 24 Oct 2017 10:04:41 GMT
```

```
ETag: "2c39-55c481153905e"
```

```
Accept-Ranges: bytes
```

```
Content-Length: 11321
```

```
Vary: Accept-Encoding
```

```
Content-Type: text/html
```

```
X-Cache: MISS from localhost
```

```
X-Cache-Lookup: MISS from localhost:3128
```

```
Connection: keep-alive
```

```
Response Body :
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

```
<html xmlns="http://www.w3.org/1999/xhtml">
```

```
<!--
```

Modified from the Debian original for Ubuntu

Last updated: 2014-03-19

See: <https://launchpad.net/bugs/1288690>

-->

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

<title>Apache2 Ubuntu Default Page: It works</title>

<style type="text/css" media="screen">

* {

margin: 0px 0px 0px 0px;

padding: 0px 0px 0px 0px;

}

body, html {

padding: 3px 3px 3px 3px;

background-color: #D8DBE2;

font-family: Verdana, sans-serif;

font-size: 11pt;

text-align: center;

}

div.main_page {

position: relative;

display: table;

width: 800px;

margin-bottom: 3px;

margin-left: auto;

margin-right: auto;

padding: 0px 0px 0px 0px;

border-width: 2px;

border-color: #212738;

border-style: solid;

background-color: #FFFFFF;

text-align: center;

}

div.page_header {

height: 99px;

width: 100%;

background-color: #F5F6F7;

}

div.page_header span {

margin: 15px 0px 0px 50px;

font-size: 180%;

font-weight: bold;

}

div.page_header img {

margin: 3px 0px 0px 40px;

border: 0px 0px 0px;

}

div.table_of_contents {

clear: left;

min-width: 200px;

margin: 3px 3px 3px 3px;

```
background-color: #FFFFFF;  
  
text-align: left;  
}  
  
div.table_of_contents_item {  
clear: left;  
  
width: 100%;  
  
[...]
```

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/80

```
Give Nessus credentials to perform local checks.
```

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:

Published: 2009/12/10, Modified: 2018/06/11

Plugin Output

tcp/80

```
Based on the response to an OPTIONS request :  
  
- HTTP methods GET HEAD OPTIONS POST are allowed on :  
  
/
```

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/80

```
URL      : http://192.168.17.1/
Version  : 2.4.99
backported : 1
os       : ConvertedUbuntu
```


192.168.17.10

0

CRITICAL

0

HIGH

0

MEDIUM

0

LOW

20

INFO

Scan Information

Start time: Tue Jun 19 10:40:12 2018

End time: Tue Jun 19 10:41:58 2018

Host Information

IP: 192.168.17.10

OS: Linux Kernel 4.4 on Ubuntu 16.04 (xenial)

Vulnerabilities

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:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

icmp/0

```
The remote clock is synchronized with the local clock.
```

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:

Published: 2003/12/09, Modified: 2018/04/19

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
Confidence level : 95
Method : SSH
```

```
The remote host is running Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
```

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:

Published: 2005/08/26, Modified: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :  
  
Nessus version : 7.1.1  
Plugin feed version : 201806151820  
Scanner edition used : Nessus  
Scan type : Normal  
Scan policy used : Basic Network Scan  
Scanner IP : 192.168.1.235  
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 : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2018/6/19 10:40 CEST
Scan duration : 106 sec
```

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:

Published: 2007/05/16, Modified: 2011/03/20

Plugin Output

tcp/0

Synopsis

It was 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/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/04/21, Modified: 2017/06/06

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:canonical:ubuntu_linux:16.04

Following application CPE's matched on the remote system :

cpe:/a:openbsd:openssh:7.2

cpe:/a:isc:bind:9.10.3:p4

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:

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 95
```

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/11/27, Modified: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.235 to 192.168.17.10 :  
192.168.1.235  
192.168.7.252  
192.168.17.10
```

```
Hop Count: 2
```


10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/10/12, Modified: 2017/12/19

Plugin Output

tcp/22

```
SSH version : SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.4
SSH supported authentication : publickey,password
SSH banner :
Ubuntu 16.04.4 LTS
```

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/03/06, Modified: 2017/05/30

Plugin Output

tcp/22

```
The remote SSH daemon supports the following versions of the
SSH protocol :
```

- 1.99
- 2.0

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/22

```
Port 22/tcp was found to be open
```

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/22

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

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22

```
Give Nessus credentials to perform local checks.
```

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22

```
Nessus negotiated the following encryption algorithm with the server :
```

```
The server supports the following options for kex_algorithms :
```

```
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha1
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
```

```
The server supports the following options for server_host_key_algorithms :
```

```
ecdsa-sha2-nistp256
rsa-sha2-256
rsa-sha2-512
ssh-ed25519
ssh-rsa
```

```
The server supports the following options for encryption_algorithms_client_to_server :
```

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

```
The server supports the following options for encryption_algorithms_server_to_client :
```

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

The server supports the following options for `mac_algorithms_client_to_server` :

```
hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
```

The server supports the following options for `mac_algorithms_server_to_client` :

```
hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
```

The server supports the following options for `compression_algorithms_client_to_server` :

```
none
```

The server supports the following options for `compression_algorithms_server_to_client` :

```
none
```

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

https://en.wikipedia.org/wiki/Domain_Name_System

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information:

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

tcp/53

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/53

```
Port 53/tcp was found to be open
```

Synopsis

Nessus was able to obtain version information on the remote DNS server.

Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.

Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2014/03/03, Modified: 2014/11/05

Plugin Output

tcp/53

```
DNS server answer for "version.bind" (over TCP) :
```

```
9.10.3-P4-Ubuntu
```

Synopsis

It is possible to obtain the version number of the remote DNS server.

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

Risk Factor

None

References

XREF OSVDB:23

Plugin Information:

Published: 1999/10/12, Modified: 2018/04/03

Plugin Output

udp/53

```
Version : 9.10.3-P4-Ubuntu
```

Synopsis

The DNS server discloses the remote host name.

Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

Risk Factor

None

Plugin Information:

Published: 2009/01/15, Modified: 2011/09/14

Plugin Output

udp/53

```
The remote host name is :  
example
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/80

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

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/80

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


192.168.17.21

7

CRITICAL

3

HIGH

18

MEDIUM

7

LOW

110

INFO

Scan Information

Start time: Tue Jun 19 10:40:12 2018

End time: Tue Jun 19 10:47:00 2018

Host Information

Netbios Name: METASPLOITABLE

IP: 192.168.17.21

OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)

Vulnerabilities

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:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -1775 seconds.
```

33850 - Unix Operating System Unsupported Version Detection

Synopsis

The operating system running on the remote host is no longer supported.

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2008/08/08, Modified: 2018/04/27

Plugin Output

tcp/0

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).  
Upgrade to Ubuntu 17.10.
```

```
For more information, see : https://wiki.ubuntu.com/Releases
```

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:

Published: 2003/12/09, Modified: 2018/04/19

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
Confidence level : 95
Method : HTTP
```

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.

```
SSH:SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
SinFP:
```

```
P1:B10113:F0x12:W5840:00204ffff:M1460:
P2:B10113:F0x12:W5792:00204ffff0402080affffff4445414401030307:M1460:
P3:B00000:F0x00:W0:00:M0
P4:70101_7_p=111R
```

```
SMTP:!:220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
SSLcert:!:i/CN:ubuntu804-base.localdomaini/O:OCOSai/OU:Office for Complication of Otherwise Simple
Affairss/CN:ubuntu804-base.localdomains/O:OCOSAs/OU:Office for Complication of Otherwise Simple
Affairs
ed093088706603bfd5dc237399b498da2d4d31c6
```

The remote host is running Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

n/a

Risk Factor

None

Plugin Information:

Published: 2005/05/15, Modified: 2017/03/13

Plugin Output

tcp/0

```
The Linux distribution detected was :  
- Ubuntu 8.04 (gutsy)
```

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:

Published: 2005/08/26, Modified: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :  
  
Nessus version : 7.1.1  
Plugin feed version : 201806151820  
Scanner edition used : Nessus  
Scan type : Normal  
Scan policy used : Basic Network Scan  
Scanner IP : 192.168.1.235  
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 : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2018/6/19 10:40 CEST
Scan duration : 408 sec
```

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:

Published: 2007/05/16, Modified: 2011/03/20

Plugin Output

tcp/0

Synopsis

It was 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/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/04/21, Modified: 2017/06/06

Plugin Output

tcp/0

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

```
cpe:/o:canonical:ubuntu_linux:8.04
```

```
Following application CPE's matched on the remote system :
```

```
cpe:/a:openbsd:openssh:4.7 -> OpenBSD OpenSSH 4.7
```

```
cpe:/a:samba:samba:3.0.20 -> Samba 3.0.20
```

```
cpe:/a:apache:http_server:2.2.8 -> Apache Software Foundation Apache HTTP Server 2.2.8
```

```
cpe:/a:php:php:5.2.4 -> PHP 5.2.4
```

```
cpe:/a:isc:bind:9.4.
```


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:

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 95
```

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:

Published: 2013/07/08, Modified: 2018/06/12

Plugin Output

tcp/0

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

```
[ Apache HTTP Server httpOnly Cookie Information Disclosure (57792) ]
```

```
+ Action to take : Upgrade to Apache version 2.0.65 / 2.2.22 or later.
```

```
[ Samba Badlock Vulnerability (90509) ]
```

```
+ Action to take : Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.
```

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/11/27, Modified: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.235 to 192.168.17.21 :  
192.168.1.235  
192.168.7.252  
192.168.17.21
```

```
Hop Count: 2
```

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:

Published: 1999/10/12, Modified: 2018/02/12

Plugin Output

tcp/21

```
The remote FTP banner is :  
  
220 (vsFTPd 2.3.4)
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/21

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

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/21

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

Synopsis

An FTP server is listening on the remote port.

Description

The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.

See Also

<http://vsftpd.beasts.org/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/03/17, Modified: 2013/03/21

Plugin Output

tcp/21

```
Source   : 220 (vsFTPd 2.3.4)
Version  : 2.3.4
```

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis

The remote SSH host keys are weak.

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

See Also

<http://www.nessus.org/u?5d01bdab>

<http://www.nessus.org/u?f14f4224>

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

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:C)

References

| | |
|------|---------------|
| BID | 29179 |
| CVE | CVE-2008-0166 |
| XREF | OSVDB:45029 |
| XREF | OSVDB:45503 |
| XREF | CWE:310 |

Exploitable With

192.168.17.21

Core Impact (true)

Plugin Information:

Published: 2008/05/14, Modified: 2017/05/30

Plugin Output

tcp/22

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

<https://tools.ietf.org/html/rfc4253#section-6.3>

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

tcp/22

```
The following weak server-to-client encryption algorithms are supported :
```

```
arcfour
arcfour128
arcfour256
```

```
The following weak client-to-server encryption algorithms are supported :
```

```
arcfour
arcfour128
arcfour256
```

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

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

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.6 (CVSS2#E:ND/RL:ND/RC:ND)

References

| | |
|------|---------------|
| BID | 32319 |
| CVE | CVE-2008-5161 |
| XREF | OSVDB:50035 |
| XREF | OSVDB:50036 |
| XREF | CERT:958563 |
| XREF | CWE:200 |

Plugin Information:

Published: 2013/10/28, Modified: 2016/05/12

Plugin Output

tcp/22

The following client-to-server Cipher Block Chaining (CBC) algorithms are supported :

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

The following server-to-client Cipher Block Chaining (CBC) algorithms are supported :

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

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

Risk Factor

Low

CVSS Base Score

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

Plugin Information:

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :
```

```
  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

```
The following server-to-client Message Authentication Code (MAC) algorithms
are supported :
```

```
  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/10/12, Modified: 2017/12/19

Plugin Output

tcp/22

```
SSH version : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
SSH supported authentication : publickey,password
```

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/03/06, Modified: 2017/05/30

Plugin Output

tcp/22

```
The remote SSH daemon supports the following versions of the  
SSH protocol :
```

- 1.99
- 2.0

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/22

```
Port 22/tcp was found to be open
```


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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/22

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

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22

```
Give Nessus credentials to perform local checks.
```

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22

```
Nessus negotiated the following encryption algorithm with the server :
```

```
The server supports the following options for kex_algorithms :
```

```
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
```

```
The server supports the following options for server_host_key_algorithms :
```

```
ssh-dss
ssh-rsa
```

```
The server supports the following options for encryption_algorithms_client_to_server :
```

```
3des-cbc
aes128-cbc
aes128-ctr
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

The server supports the following options for encryption_algorithms_server_to_client :

```
3des-cbc
aes128-cbc
aes128-ctr
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

The server supports the following options for mac_algorithms_client_to_server :

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
umac-64@openssh.com
```

The server supports the following options for mac_algorithms_server_to_client :

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
umac-64@openssh.com
```

The server supports the following options for compression_algorithms_client_to_server :

```
none
zlib@openssh.com
```

The server supports the following options for compression_algorithms_server_to_client :

```
none
zlib@openssh.com
```



```
metasploitable login:
```

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

Synopsis

A Telnet server is listening on the remote port.

| Description |
|-------------|
| |

The remote host is running a Telnet server, a remote terminal server.

Solution

Disable this service if you do not use it.

| Risk Factor | Impact | Control |
|--------------------------------------|--------|-----------------------------------|
| 1. Market Volatility | High | 1. Diversification of investments |
| 2. Interest Rate Fluctuations | Medium | 2. Hedging strategies |
| 3. Regulatory Changes | Medium | 3. Compliance monitoring |
| 4. Operational Risks | Low | 4. Robust internal controls |
| 5. Counterparty Risk | Medium | 5. Credit rating monitoring |
| 6. Systemic Risk | High | 6. Stress testing |
| 7. Liquidity Risk | Medium | 7. Liquidity management |
| 8. Reputation Risk | Medium | 8. Proactive communication |
| 9. Environmental Risk | Low | 9. Sustainability reporting |
| 10. Human Capital Risk | Medium | 10. Employee training |

None

Plugin Information:

Published: 1999/10/12, Modified: 2018/02/12

Plugin Output

tcp/23

[illegible][illegible][illegible][illegible][illegible][illegible][illegible]

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/23

```
Port 23/tcp was found to be open
```


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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/23

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

Synopsis

The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

See Also

<http://www.nessus.org/u?5d01bdab>

<http://www.nessus.org/u?f14f4224>

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

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:C)

References

| | |
|------|---------------|
| BID | 29179 |
| CVE | CVE-2008-0166 |
| XREF | OSVDB:45029 |
| XREF | OSVDB:45503 |
| XREF | CWE:310 |

Exploitable With

192.168.17.21

Core Impact (true)

Plugin Information:

Published: 2008/05/15, Modified: 2015/10/07

Plugin Output

tcp/25

Synopsis

The remote server's SSL certificate has already expired.

Description

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

Solution

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

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2004/12/03, Modified: 2016/01/08

Plugin Output

tcp/25

```
The SSL certificate has already expired :
```

```
  Subject      : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
emailAddress=root@ubuntu804-base.localdomain
  Issuer       : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA,
OU=Office for Complication of Otherwise Simple Affairs, CN=ubuntu804-base.localdomain,
emailAddress=root@ubuntu804-base.localdomain
  Not valid before : Mar 17 14:07:45 2010 GMT
  Not valid after  : Apr 16 14:07:45 2010 GMT
```

Synopsis

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

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>

<http://www.nessus.org/u?0bb7b67d>

<http://www.nessus.org/u?247c4540>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<http://www.nessus.org/u?5d15ba70>

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://tools.ietf.org/html/rfc7507>

<https://tools.ietf.org/html/rfc7568>

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.1 (with approved cipher suites) or higher instead.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2005/10/12, Modified: 2017/07/11

Plugin Output

tcp/25

```
- SSLv3 is enabled and the server supports at least one cipher.
```

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

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

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

See Also

<http://www.nessus.org/u?6527892d>

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

References

| | |
|------|---------|
| XREF | CWE:326 |
| XREF | CWE:327 |
| XREF | CWE:720 |
| XREF | CWE:753 |
| XREF | CWE:803 |
| XREF | CWE:928 |
| XREF | CWE:934 |

Plugin Information:

Published: 2007/10/08, Modified: 2018/05/16

Plugin Output

192.168.17.21

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

Low Strength Ciphers (<= 64-bit key)

| | | | | |
|-------------------------|-------------|---------|-----------------|----------|
| EXP-EDH-RSA-DES-CBC-SHA | Kx=DH(512) | Au=RSA | Enc=DES-CBC(40) | Mac=SHA1 |
| export | | | | |
| EDH-RSA-DES-CBC-SHA | Kx=DH | Au=RSA | Enc=DES-CBC(56) | Mac=SHA1 |
| EXP-ADH-DES-CBC-SHA | Kx=DH(512) | Au=None | Enc=DES-CBC(40) | Mac=SHA1 |
| export | | | | |
| EXP-ADH-RC4-MD5 | Kx=DH(512) | Au=None | Enc=RC4(40) | Mac=MD5 |
| export | | | | |
| ADH-DES-CBC-SHA | Kx=DH | Au=None | Enc=DES-CBC(56) | Mac=SHA1 |
| EXP-DES-CBC-SHA | Kx=RSA(512) | Au=RSA | Enc=DES-CBC(40) | Mac=SHA1 |
| export | | | | |
| EXP-RC2-CBC-MD5 | Kx=RSA(512) | Au=RSA | Enc=RC2-CBC(40) | Mac=MD5 |
| export | | | | |
| EXP-RC4-MD5 | Kx=RSA(512) | Au=RSA | Enc=RC4(40) | Mac=MD5 |
| export | | | | |
| DES-CBC-SHA | Kx=RSA | Au=RSA | Enc=DES-CBC(56) | Mac=SHA1 |

The fields above are :

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


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. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

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

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

tcp/25

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

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

| | | | | |
|----------------------|--------|---------|-------------------|----------|
| EDH-RSA-DES-CBC3-SHA | Kx=DH | Au=RSA | Enc=3DES-CBC(168) | Mac=SHA1 |
| ADH-DES-CBC3-SHA | Kx=DH | Au=None | 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) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/25

```
The identities known by Nessus are :
```

```
192.168.17.21
192.168.17.21
```

```
The Common Name in the certificate is :
```

```
ubuntu804-base.localdomain
```

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that 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.

See Also

<http://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/25

The following certificate was part of the certificate chain sent by the remote host, but it has expired :

```
| -Subject    : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for  
Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-  
base.localdomain  
| -Not After  : Apr 16 14:07:45 2010 GMT
```

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

```
| -Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for  
Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-  
base.localdomain  
| -Issuer  : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for  
Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-  
base.localdomain
```

Synopsis

The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.

Description

The remote SMTP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase.

Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials.

See Also

<https://tools.ietf.org/html/rfc2487>

<http://www.securityfocus.com/archive/1/516901/30/0/threaded>

Solution

Contact the vendor to see if an update is available.

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 | 46767 |
| CVE | CVE-2011-0411 |
| CVE | CVE-2011-1430 |
| CVE | CVE-2011-1431 |
| CVE | CVE-2011-1432 |
| CVE | CVE-2011-1506 |
| CVE | CVE-2011-2165 |
| XREF | OSVDB:71020 |
| XREF | OSVDB:71021 |

| | |
|------|-------------|
| XREF | OSVDB:71854 |
| XREF | OSVDB:71946 |
| XREF | OSVDB:73251 |
| XREF | OSVDB:75014 |
| XREF | OSVDB:75256 |
| XREF | CERT:555316 |

Plugin Information:

Published: 2011/03/10, Modified: 2017/06/12

Plugin Output

tcp/25

```
Nessus sent the following two commands in a single packet :
```

```
STARTTLS\r\nRESET\r\n
```

```
And the server sent the following two responses :
```

```
220 2.0.0 Ready to start TLS
250 2.0.0 Ok
```

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:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/25

```
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 : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
Complication of Otherwise Simple Affairs/CN=ubuntu804-base.localdomain/E=root@ubuntu804-
base.localdomain
```


Synopsis

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

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

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

See Also

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00>

Solution

Disable SSLv3.

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

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

| | |
|------|---------------|
| BID | 70574 |
| CVE | CVE-2014-3566 |
| XREF | OSVDB:113251 |
| XREF | CERT:577193 |

Plugin Information:

Published: 2014/10/15, Modified: 2016/11/30

Plugin Output

tcp/25

Nessus determined that the remote server supports SSLv3 with at least one CBC cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the Fallback SCSV mechanism is not supported, allowing connections to be "rolled back" to SSLv3.

81606 - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.

See Also

<https://www.smacktls.com/#freak>

<https://www.openssl.org/news/secadv/20150108.txt>

<http://www.nessus.org/u?b78da2c4>

Solution

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

| | |
|------|---------------|
| BID | 71936 |
| CVE | CVE-2015-0204 |
| XREF | OSVDB:116794 |
| XREF | CERT:243585 |

Plugin Information:

Published: 2015/03/04, Modified: 2018/05/21

Plugin Output

tcp/25

EXPORT_RSA cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

| | | | | |
|---------------------------|-------------|--------|-----------------|----------|
| EXP-DES-CBC-SHA
export | Kx=RSA(512) | Au=RSA | Enc=DES-CBC(40) | Mac=SHA1 |
| EXP-RC2-CBC-MD5
export | Kx=RSA(512) | Au=RSA | Enc=RC2-CBC(40) | Mac=MD5 |
| EXP-RC4-MD5
export | Kx=RSA(512) | Au=RSA | Enc=RC4(40) | Mac=MD5 |

The fields above are :

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

31705 - SSL Anonymous Cipher Suites Supported

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

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

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

See Also

<http://www.nessus.org/u?3a040ada>

Solution

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

Risk Factor

Low

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/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

2.3 (CVSS2#E:ND/RL:OF/RC:C)

References

| | |
|------|---------------|
| BID | 28482 |
| CVE | CVE-2007-1858 |
| XREF | OSVDB:34882 |

Plugin Information:

Published: 2008/03/28, Modified: 2018/01/29

Plugin Output

tcp/25

The following is a list of SSL anonymous ciphers supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

| | | | | |
|---------------------|------------|---------|-----------------|----------|
| EXP-ADH-DES-CBC-SHA | Kx=DH(512) | Au=None | Enc=DES-CBC(40) | Mac=SHA1 |
| export | | | | |
| EXP-ADH-RC4-MD5 | Kx=DH(512) | Au=None | Enc=RC4(40) | Mac=MD5 |
| export | | | | |
| ADH-DES-CBC-SHA | Kx=DH | Au=None | Enc=DES-CBC(56) | Mac=SHA1 |

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

| | | | | |
|------------------|-------|---------|-------------------|----------|
| ADH-DES-CBC3-SHA | Kx=DH | Au=None | Enc=3DES-CBC(168) | Mac=SHA1 |
|------------------|-------|---------|-------------------|----------|

High Strength Ciphers (>= 112-bit key)

| | | | | |
|----------------|-------|---------|------------------|----------|
| ADH-AES128-SHA | Kx=DH | Au=None | Enc=AES-CBC(128) | Mac=SHA1 |
| ADH-AES256-SHA | Kx=DH | Au=None | Enc=AES-CBC(256) | Mac=SHA1 |
| ADH-RC4-MD5 | Kx=DH | Au=None | Enc=RC4(128) | Mac=MD5 |

The fields above are :

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

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:

Published: 2013/04/05, Modified: 2018/05/21

Plugin Output

tcp/25

List of RC4 cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

| | | | | |
|-----------------|-------------|---------|-------------|---------|
| EXP-ADH-RC4-MD5 | Kx=DH(512) | Au=None | Enc=RC4(40) | Mac=MD5 |
| export | | | | |
| EXP-RC4-MD5 | Kx=RSA(512) | Au=RSA | Enc=RC4(40) | Mac=MD5 |
| export | | | | |

High Strength Ciphers (>= 112-bit key)

| | | | | |
|-------------|--------|---------|--------------|----------|
| ADH-RC4-MD5 | Kx=DH | Au=None | Enc=RC4(128) | Mac=MD5 |
| 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}

83738 - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.

See Also

<https://weakdh.org/>

Solution

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.2 (CVSS2#E:F/RL:TF/RC:ND)

References

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

Plugin Information:

Published: 2015/05/21, Modified: 2016/06/16

Plugin Output

tcp/25

EXPORT_DHE cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

| | | | | |
|-------------------------|------------|---------|-----------------|----------|
| EXP-EDH-RSA-DES-CBC-SHA | Kx=DH(512) | Au=RSA | Enc=DES-CBC(40) | Mac=SHA1 |
| export | | | | |
| EXP-ADH-DES-CBC-SHA | Kx=DH(512) | Au=None | Enc=DES-CBC(40) | Mac=SHA1 |
| export | | | | |
| EXP-ADH-RC4-MD5 | Kx=DH(512) | Au=None | Enc=RC4(40) | Mac=MD5 |
| export | | | | |

The fields above are :

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

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 v3.0 Base Score

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

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:

Published: 2015/05/28, Modified: 2018/05/21

Plugin Output

tcp/25

Vulnerable connection combinations :

SSL/TLS version : TLSv1.0
Cipher suite : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Diffie-Hellman MODP size (bits) : 512
Logjam attack difficulty : Easy (could be carried out by individuals)

SSL/TLS version : SSLv3
Cipher suite : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Diffie-Hellman MODP size (bits) : 512
Logjam attack difficulty : Easy (could be carried out by individuals)

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:

Published: 1999/10/12, Modified: 2011/03/11

Plugin Output

tcp/25

```
Remote SMTP server banner :  
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

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:

Published: 2008/05/19, Modified: 2015/12/30

Plugin Output

tcp/25

```
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
            7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
            73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
            D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
            8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
            98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
            00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
            0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
            1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
            68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
            83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
            A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
            15 6E 8D 30 38 F6 CA 2E 75

Fingerprints :

SHA-256 Fingerprint: E7 A7 FA 0D 63 E4 57 C7 C4 A5 9B 38 B7 08 49 C6 A7 0B DA 6F
                    83 0C 7A F1 E3 2D EE 43 6D E8 13 CC
SHA-1 Fingerprint: ED 09 30 88 70 66 03 BF D5 DC 23 73 99 B4 98 DA 2D [...]
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/25

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


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/man1.1.0/apps/ciphers.html>

<http://www.nessus.org/u?3a040ada>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/03/29

Plugin Output

tcp/25

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

SSL Version : TLSv1

Low Strength Ciphers (<= 64-bit key)

| | | | | |
|-------------------------|-------------|---------|-----------------|----------|
| EXP-EDH-RSA-DES-CBC-SHA | Kx=DH(512) | Au=RSA | Enc=DES-CBC(40) | Mac=SHA1 |
| export | | | | |
| EDH-RSA-DES-CBC-SHA | Kx=DH | Au=RSA | Enc=DES-CBC(56) | Mac=SHA1 |
| EXP-ADH-DES-CBC-SHA | Kx=DH(512) | Au=None | Enc=DES-CBC(40) | Mac=SHA1 |
| export | | | | |
| EXP-ADH-RC4-MD5 | Kx=DH(512) | Au=None | Enc=RC4(40) | Mac=MD5 |
| export | | | | |
| ADH-DES-CBC-SHA | Kx=DH | Au=None | Enc=DES-CBC(56) | Mac=SHA1 |
| EXP-DES-CBC-SHA | Kx=RSA(512) | Au=RSA | Enc=DES-CBC(40) | Mac=SHA1 |
| export | | | | |
| EXP-RC2-CBC-MD5 | Kx=RSA(512) | Au=RSA | Enc=RC2-CBC(40) | Mac=MD5 |
| export | | | | |
| EXP-RC4-MD5 | Kx=RSA(512) | Au=RSA | Enc=RC4(40) | Mac=MD5 |
| export | | | | |
| DES-CBC-SHA | Kx=RSA | Au=RSA | Enc=DES-CBC(56) | Mac=SHA1 |

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

| | | | | |
|----------------------|--------|---------|-------------------|----------|
| EDH-RSA-DES-CBC3-SHA | Kx=DH | Au=RSA | Enc=3DES-CBC(168) | Mac=SHA1 |
| ADH-DES-CBC3-SHA | Kx=DH | Au=None | 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 |
| ADH-AES128-SHA | Kx=DH | Au=None | Enc=AES-CBC(128) | Mac=SHA1 |
| ADH-AES256-SHA | Kx=DH | Au=None | Enc=AES-CBC(256) | Mac=SHA1 |
| ADH-RC4-MD5 | Kx=DH | Au=None | Enc=RC4(128) | Mac=MD5 |
| AES128-SHA | Kx=RSA | Au=RSA | [...] | |

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/25

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

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

<https://en.wikipedia.org/wiki/STARTTLS>

<https://tools.ietf.org/html/rfc2487>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/10/09, Modified: 2017/06/15

Plugin Output

tcp/25

```
Here is the SMTP service's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :
```

```
----- snip -----
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
```

```
Common Name: ubuntu804-base.localdomain
Email Address: root@ubuntu804-base.localdomain

Serial Number: 00 FA F9 3A 4C 7F B6 B9 CC

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 17 14:07:45 2010 GMT
Not Valid After: Apr 16 14:07:45 2010 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 D6 B4 13 36 33 9A 95 71 7B 1B DE 7C 83 75 DA 71 B1 3C A9
             7F FE AD 64 1B 77 E9 4F AE BE CA D4 F8 CB EF AE BB 43 79 24
             73 FF 3C E5 9E 3B 6D FC C8 B1 AC FA 4C 4D 5E 9B 4C 99 54 0B
             D7 A8 4A 50 BA A9 DE 1D 1F F4 E4 6B 02 A3 F4 6B 45 CD 4C AF
             8D 89 62 33 8F 65 BB 36 61 9F C4 2C 73 C1 4E 2E A0 A8 14 4E
             98 70 46 61 BB D1 B9 31 DF 8C 99 EE 75 6B 79 3C 40 A0 AE 97
             00 90 9D DC 99 0D 33 A4 B5
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 92 A4 B4 B8 14 55 63 25 51 4A 0B C3 2A 22 CF 3A F8 17 6A
           0C CF 66 AA A7 65 2F 48 6D CD E3 3E 5C 9F 77 6C D4 44 54 1F
           1E 84 4F 8E D4 8D DD AC 2D 88 09 21 A8 DA 56 2C A9 05 3C 49
           68 35 19 75 0C DA 53 23 88 88 19 2D 74 26 C1 22 65 EE 11 68
           83 6A 53 4A 9C 27 CB A0 B4 E9 8D 29 0C B2 3C 18 5C 67 CC 53
           A6 1E 30 D0 AA 26 7B 1E AE 40 B9 29 01 6C 2E BC A2 19 94 7C
           15 6E 8D 30 38 F6 CA 2E 75

----- snip ----- [...]
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

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

Risk Factor

None

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/25

```
The host name known by Nessus is :
```

```
metasploitable
```

```
The Common Name in the certificate is :
```

```
ubuntu804-base.localdomain
```

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:

Published: 2010/11/30, Modified: 2013/10/18

Plugin Output

tcp/25

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:

Published: 2011/02/07, Modified: 2013/10/18

Plugin Output

tcp/25

```
This port supports resuming SSLv3 sessions.
```


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:

Published: 2011/12/01, Modified: 2018/02/15

Plugin Output

tcp/25

```
This port supports SSLv3/TLSv1.0.
```

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>

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/12/07, Modified: 2017/06/12

Plugin Output

tcp/25

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

Low Strength Ciphers (<= 64-bit key)

| | | | | |
|-------------------------|------------|--------|-----------------|----------|
| EXP-EDH-RSA-DES-CBC-SHA | Kx=DH(512) | Au=RSA | Enc=DES-CBC(40) | Mac=SHA1 |
| export | | | | |
| EDH-RSA-DES-CBC-SHA | Kx=DH | Au=RSA | Enc=DES-CBC(56) | Mac=SHA1 |

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

| | | | | |
|----------------------|-------|--------|-------------------|----------|
| EDH-RSA-DES-CBC3-SHA | Kx=DH | 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 |

The fields above are :

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

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

<http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml>

<https://tools.ietf.org/html/rfc3749>

<https://tools.ietf.org/html/rfc3943>

<https://tools.ietf.org/html/rfc5246>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2012/10/16, Modified: 2018/02/15

Plugin Output

tcp/25

```
Nessus was able to confirm that the following compression method is
supported by the target :
```

```
DEFLATE (0x01)
```

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:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/25

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

Low Strength Ciphers (<= 64-bit key)

| | | | | | |
|--------|-------------------------|-------------|---------|-----------------|----------|
| export | EXP-EDH-RSA-DES-CBC-SHA | Kx=DH(512) | Au=RSA | Enc=DES-CBC(40) | Mac=SHA1 |
| | EDH-RSA-DES-CBC-SHA | Kx=DH | Au=RSA | Enc=DES-CBC(56) | Mac=SHA1 |
| export | EXP-ADH-DES-CBC-SHA | Kx=DH(512) | Au=None | Enc=DES-CBC(40) | Mac=SHA1 |
| | ADH-DES-CBC-SHA | Kx=DH | Au=None | Enc=DES-CBC(56) | Mac=SHA1 |
| export | EXP-DES-CBC-SHA | Kx=RSA(512) | Au=RSA | Enc=DES-CBC(40) | Mac=SHA1 |
| export | EXP-RC2-CBC-MD5 | Kx=RSA(512) | Au=RSA | Enc=RC2-CBC(40) | Mac=MD5 |
| | DES-CBC-SHA | Kx=RSA | Au=RSA | Enc=DES-CBC(56) | Mac=SHA1 |

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

| | | | | |
|----------------------|--------|---------|-------------------|----------|
| EDH-RSA-DES-CBC3-SHA | Kx=DH | Au=RSA | Enc=3DES-CBC(168) | Mac=SHA1 |
| ADH-DES-CBC3-SHA | Kx=DH | Au=None | 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 |
| ADH-AES128-SHA | Kx=DH | Au=None | Enc=AES-CBC(128) | Mac=SHA1 |
| ADH-AES256-SHA | Kx=DH | Au=None | 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}
```

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2018/04/24

Plugin Output

tcp/25

```
TLSv1 is enabled and the server supports at least one cipher.
```

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

https://en.wikipedia.org/wiki/Domain_Name_System

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Plugin Information:

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

tcp/53

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/53

```
Port 53/tcp was found to be open
```

Synopsis

Nessus was able to obtain version information on the remote DNS server.

Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.

Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2014/03/03, Modified: 2014/11/05

Plugin Output

tcp/53

```
DNS server answer for "version.bind" (over TCP) :  
  
9.4.2
```

Synopsis

It is possible to obtain the version number of the remote DNS server.

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

Risk Factor

None

References

XREF OSVDB:23

Plugin Information:

Published: 1999/10/12, Modified: 2018/04/03

Plugin Output

udp/53

```
Version : 9.4.2
```

Synopsis

The DNS server discloses the remote host name.

Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

Risk Factor

None

Plugin Information:

Published: 2009/01/15, Modified: 2011/09/14

Plugin Output

udp/53

```
The remote host name is :  
metasploitable
```

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:

Published: 2003/01/23, Modified: 2018/05/21

Plugin Output

tcp/80

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 /Nessus773958362.html HTTP/1.1
Connection: Close
Host: 192.168.17.21
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: Tue, 19 Jun 2018 09:14:28 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Content-Type: message/http
X-Cache: MISS from localhost
X-Cache-Lookup: NONE from localhost:3128
Transfer-Encoding: chunked
Connection: keep-alive

TRACE /Nessus773958362.html HTTP/1.1
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
Host: 192.168.17.21
X-Forwarded-For: 192.168.1.235
```

```
Cache-Control: max-age=259200  
Connection: keep-alive
```

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

Synopsis

The web server running on the remote host is affected by an information disclosure vulnerability.

Description

The version of Apache HTTP Server running on the remote host is affected by an information disclosure vulnerability. Sending a request with HTTP headers long enough to exceed the server limit causes the web server to respond with an HTTP 400. By default, the offending HTTP header and value are displayed on the 400 error page. When used in conjunction with other attacks (e.g., cross-site scripting), this could result in the compromise of httpOnly cookies.

See Also

http://fd.the-wildcat.de/apache_e36a9cf46c.php

<http://www.nessus.org/u?e005199a>

http://httpd.apache.org/security/vulnerabilities_22.html

<http://svn.apache.org/viewvc?view=revision&revision=1235454>

Solution

Upgrade to Apache version 2.0.65 / 2.2.22 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

3.4 (CVSS2#E:POC/RL:OF/RC:C)

References

| | |
|------|---------------|
| BID | 51706 |
| CVE | CVE-2012-0053 |
| XREF | OSVDB:78556 |
| XREF | EDB-ID:18442 |

Plugin Information:

Published: 2012/02/02, Modified: 2017/04/28

Plugin Output

tcp/80

Nessus verified this by sending a request with a long Cookie header :

```
GET / HTTP/1.1
Host: 192.168.17.21
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

Which caused the Cookie header to be displayed in the default error page
(the response shown below has been truncated) :

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
Size of a request header field exceeds server limit.<br />
<pre>
Cookie: z9=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
```

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:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/80

```
The remote web server type is :  
Apache/2.2.8 (Ubuntu) DAV/2
```

Synopsis

A transparent or reverse HTTP proxy is running on this port.

Description

This web server is reachable through a reverse HTTP proxy.

Solution

n/a

Risk Factor

None

References

| | |
|------|---------------|
| CVE | CVE-2004-2320 |
| CVE | CVE-2005-3398 |
| CVE | CVE-2005-3498 |
| CVE | CVE-2007-3008 |
| XREF | OSVDB:877 |
| XREF | OSVDB:3726 |
| XREF | OSVDB:35511 |
| XREF | OSVDB:50485 |
| XREF | CWE:200 |
| XREF | CWE:79 |

Plugin Information:

Published: 2002/07/02, Modified: 2018/05/21

Plugin Output

tcp/80

```
There might be a caching proxy on the way to this web server:
MISS from localhost
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/80

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

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/80

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

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

| Risk Factor | Impact | Control |
|--------------------------------------|--------|------------------------------|
| 1. Market Volatility | High | 1. Diversification of assets |
| 2. Interest Rate Fluctuations | Medium | 2. Hedging strategies |
| 3. Credit Default Risk | Medium | 3. Credit rating agencies |
| 4. Liquidity Constraints | Medium | 4. Liquidity management |
| 5. Regulatory Changes | Medium | 5. Compliance monitoring |
| 6. Operational Risks | Low | 6. Internal controls |
| 7. Reputation Risk | Low | 7. PR management |
| 8. Geopolitical Tensions | Medium | 8. Geopolitical analysis |
| 9. Technological Disruption | Medium | 9. Innovation investment |
| 10. Environmental Risks | Medium | 10. ESG integration |

None

Plugin Information:

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/80

Response Code : HTTP/1.1 200 OK

```
Protocol version : HTTP/1.1
```

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Date: Tue, 19 Jun 2018 09:14:25 GMT

Server: Apache/2.2.8 (Ubuntu) DAV/2

X-Powered-By: PHP/5.2.4-2ubuntu5.10

Content-Length: 891

Content-Type: text/html

```
X-Cache: MISS from localhost
```

```
X-Cache-Lookup: MISS from localhost:3128
```

Connection: keep-alive

Response Body :

```
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
```

[illegible]

|_ |

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

```
</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
```

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/80

```
Give Nessus credentials to perform local checks.
```


Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/80

```
URL      : http://192.168.17.21/
Version  : 2.2.99
backported : 1
modules  : DAV/2
os       : ConvertedUbuntu
```

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/08/04, Modified: 2017/07/07

Plugin Output

tcp/80

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

```
Version : 5.2.4-2ubuntu5.10
```

```
Source  : X-Powered-By: PHP/5.2.4-2ubuntu5.10
```

84574 - Backported Security Patch Detection (PHP)

Synopsis

Security patches have been backported.

Description

Security patches may have been 'backported' to the remote PHP install without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2015/07/07, Modified: 2015/07/07

Plugin Output

tcp/80

```
Give Nessus credentials to perform local checks.
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/111

```
Port 111/tcp was found to be open
```

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/04/08, Modified: 2011/08/29

Plugin Output

tcp/111

10223 - RPC portmapper Service Detection

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

Solution

n/a

Risk Factor

None

References

CVE CVE-1999-0632

Plugin Information:

Published: 1999/08/19, Modified: 2014/02/19

Plugin Output

udp/111

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/111

```
The following RPC services are available on UDP port 111 :  
- program: 100000 (portmapper), version: 2
```

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:

Published: 1999/10/12, Modified: 2018/06/06

Plugin Output

udp/137

```
The following 5 NetBIOS names have been gathered :
```

```
METASPLOITABLE = Computer name
METASPLOITABLE = Messenger Service
METASPLOITABLE = File Server Service
WORKGROUP      = Workgroup / Domain name
WORKGROUP      = Browser Service Elections
```

```
This SMB server seems to be a Samba server - its MAC address is NULL.
```


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:

Published: 2002/06/05, Modified: 2015/06/02

Plugin Output

tcp/139

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

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/139

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

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 v3.0 Base Score

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

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

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:

Published: 2012/01/19, Modified: 2018/05/02

Plugin Output

tcp/445

Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability.

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists 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 who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

See Also

<http://badlock.org>

<https://www.samba.org/samba/security/CVE-2016-2118.html>

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	86002
CVE	CVE-2016-2118
XREF	OSVDB:136339
XREF	CERT:813296

Plugin Information:

Published: 2016/04/13, Modified: 2016/07/25

Plugin Output

tcp/445

Nessus detected that the Samba Badlock patch has not been applied.

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

<https://support.microsoft.com/kb/143474>

<https://support.microsoft.com/kb/246261>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/05/09, Modified: 2018/06/06

Plugin Output

tcp/445

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

Synopsis

It is possible to obtain network information.

Description

It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Solution

n/a

Risk Factor

None

References

XREF OSVDB:300

Plugin Information:

Published: 2000/05/09, Modified: 2015/01/12

Plugin Output

tcp/445

```
Here is the browse list of the remote host :
```

```
METASPLOITABLE ( os : 0.0 )  
TST-WXP-BUILD26 ( os : 0.0 )
```


Synopsis

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

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/10/17, Modified: 2017/11/30

Plugin Output

tcp/445

```
The remote Operating System is : Unix
The remote native LAN manager is : Samba 3.0.20-Debian
The remote SMB Domain Name is : METASPLOITABLE
```

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:

Published: 2002/06/05, Modified: 2015/06/02

Plugin Output

tcp/445

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

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/445

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

Synopsis

An SMB server is running on the remote host.

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

See Also

<http://www.samba.org/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/05/16, Modified: 2013/01/07

Plugin Output

tcp/445

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

<https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>

<https://support.microsoft.com/en-us/kb/2696547>

<http://www.nessus.org/u?8dcab5e4>

<http://www.nessus.org/u?36fd3072>

<http://www.nessus.org/u?4c7e0cf3>

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF OSVDB:151058

Plugin Information:

Published: 2017/02/03, Modified: 2017/02/16

Plugin Output

tcp/445

```
The remote host supports SMBv1.
```

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2017/06/19, Modified: 2017/06/19

Plugin Output

tcp/445

```
The remote host supports the following versions of SMB :  
SMBv1
```

Synopsis

It was possible to obtain the samba version from the remote operating system.

Description

Nessus was able to obtain the samba version from the remote operating by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2017/11/30, Modified: 2017/11/30

Plugin Output

tcp/445

```
The remote Samba Version is : Samba 3.0.20-Debian
```

Synopsis

It was possible to obtain information about the dialects of SMB2 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/02/09, Modified: 2018/02/09

Plugin Output

tcp/445

```
The remote host does NOT support the following SMB dialects :
 _version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.0        Windows 8
3.0.2      Windows 8.1
3.1        Windows 10
3.1.1      Windows 10
```


Synopsis

The rexecd service is running on the remote host.

Description

The rexecd service is running on the remote host. This service is design to allow users of a network to execute commands remotely.

However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third-party host.

Solution

Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

Risk Factor

Critical

CVSS Base Score

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

References

CVE	CVE-1999-0618
XREF	OSVDB:9721

Plugin Information:

Published: 1999/08/31, Modified: 2016/01/05

Plugin Output

tcp/512

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/512

```
Port 512/tcp was found to be open
```

Synopsis

The rlogin service is running on the remote host.

Description

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.

Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-1999-0651
XREF	OSVDB:193

Exploitable With

Metasploit (true)

Plugin Information:

Published: 1999/08/30, Modified: 2016/01/05

Plugin Output

tcp/513

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/513

```
Port 513/tcp was found to be open
```

Synopsis

The rsh service is running on the remote host.

Description

The rsh service is running on the remote host. This service is vulnerable since data is passed between the rsh client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication.

Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

Solution

Comment out the 'rsh' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Risk Factor

High

CVSS Base Score

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

References

CVE	CVE-1999-0651
XREF	OSVDB:193

Exploitable With

Metasploit (true)

Plugin Information:

Published: 1999/08/22, Modified: 2016/01/05

Plugin Output

tcp/514

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/514

```
Port 514/tcp was found to be open
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/1099

```
Port 1099/tcp was found to be open
```

Synopsis

An RMI registry is listening on the remote host.

Description

The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.

See Also

<http://docs.oracle.com/javase/1.5.0/docs/guide/rmi/spec/rmiTOC.html>

<http://www.nessus.org/u?eb68319f>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/08/16, Modified: 2016/04/20

Plugin Output

tcp/1099

51988 - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

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)

Plugin Information:

Published: 2011/02/15, Modified: 2018/05/16

Plugin Output

tcp/1524

```
Nessus was able to execute the command "id" using the
following request :
```

```
This produced the following truncated output (limited to 10 lines) :
----- snip -----
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
----- snip -----
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/1524

```
Port 1524/tcp was found to be open
```

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/1524

```
A shell server (Metasploitable) is running on this port.
```

Synopsis

The remote NFS server exports world-readable shares.

Description

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

See Also

<http://www.tldp.org/HOWTO/NFS-HOWTO/security.html>

Solution

Place the appropriate restrictions on all NFS shares.

Risk Factor

Medium

CVSS Base Score

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

References

XREF OSVDB:339

Plugin Information:

Published: 2009/10/26, Modified: 2016/11/23

Plugin Output

tcp/2049

```
The following shares have no access restrictions :  
  
/ *
```

Synopsis

The remote NFS server exports a list of shares.

Description

This plugin retrieves the list of NFS exported shares.

See Also

<http://www.tldp.org/HOWTO/NFS-HOWTO/security.html>

Solution

Ensure each share is intended to be exported.

Risk Factor

None

References

CVE	CVE-1999-0554
XREF	OSVDB:339

Plugin Information:

Published: 2000/06/07, Modified: 2018/05/21

Plugin Output

tcp/2049

```
Here is the export list of 192.168.17.21 :  
  
/ *
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/2049

```
Port 2049/tcp was found to be open
```

11356 - NFS Exported Share Information Disclosure

Synopsis

It is possible to access NFS shares on the remote host.

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Risk Factor

Critical

CVSS Base Score

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

References

CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554
XREF	OSVDB:339
XREF	OSVDB:8750
XREF	OSVDB:11516

Exploitable With

Metasploit (true)

Plugin Information:

Published: 2003/03/12, Modified: 2018/05/21

Plugin Output

udp/2049

```
The following NFS shares could be mounted :
```

```
+ /  
+ Contents of / :
```

```
- .  
- ..  
- bin  
- boot  
- cdrom  
- dev  
- etc  
- home  
- initrd  
- initrd.img  
- lib  
- lost+found  
- media  
- mnt  
- nohup.out  
- opt  
- proc  
- root  
- sbin  
- srv  
- sys  
- tmp  
- usr  
- var  
- vmlinuz
```


Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/2049

```
The following RPC services are available on UDP port 2049 :
```

- program: 100003 (nfs), version: 2
- program: 100003 (nfs), version: 3
- program: 100003 (nfs), version: 4

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/2121

```
Port 2121/tcp was found to be open
```

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MySQL, an open source database server.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/13, Modified: 2013/01/07

Plugin Output

tcp/3306

```
Version   : 5.0.51a-3ubuntu5
Protocol  : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_SSL (Switch to SSL after handshake)
  CLIENT_TRANSACTIONS (Client knows about transactions)
  CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```

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:

Published: 2002/11/18, Modified: 2017/06/08

Plugin Output

tcp/3306

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

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/3306

```
Port 3306/tcp was found to be open
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/3632

```
Port 3632/tcp was found to be open
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/5432

```
Port 5432/tcp was found to be open
```

Synopsis

A database service is listening on the remote host.

Description

The remote service is a PostgreSQL database server, or a derivative such as EnterpriseDB.

See Also

<http://www.postgresql.org/>

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information:

Published: 2007/09/14, Modified: 2013/02/14

Plugin Output

tcp/5432

61708 - VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak password.

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Risk Factor

Critical

CVSS Base Score

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

Plugin Information:

Published: 2012/08/29, Modified: 2015/09/24

Plugin Output

tcp/5900

```
Nessus logged in using a password of "password".
```

Synopsis

The remote host is running a remote display software (VNC).

Description

The remote host is running VNC (Virtual Network Computing), which uses the RFB (Remote Framebuffer) protocol to provide remote access to graphical user interfaces and thus permits a console on the remote host to be displayed on another.

See Also

<https://en.wikipedia.org/wiki/Vnc>

Solution

Make sure use of this software is done in accordance with your organization's security policy and filter incoming traffic to this port.

Risk Factor

None

Plugin Information:

Published: 2000/03/07, Modified: 2017/06/12

Plugin Output

tcp/5900

```
The highest RFB protocol version supported by the server is :  
3.3
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/5900

```
Port 5900/tcp was found to be open
```

19288 - VNC Server Security Type Detection

Synopsis

A VNC server is running on the remote host.

Description

This script checks the remote VNC server protocol version and the available 'security types'.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2005/07/22, Modified: 2014/03/12

Plugin Output

tcp/5900

```
The remote VNC server chose security type #2 (VNC authentication)
```

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/5900

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

Synopsis

A VNC server with one or more unencrypted 'security-types' is running on the remote host.

Description

This script checks the remote VNC server protocol version and the available 'security types' to determine if any unencrypted 'security-types' are in use or available.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/04/03, Modified: 2014/03/12

Plugin Output

tcp/5900

```
The remote VNC server supports the following security type
which does not perform full data communication encryption :
```

```
  2 (VNC authentication)
```

10407 - X Server Detection

Synopsis

An X11 server is listening on the remote host

Description

The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client.

Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

Solution

Restrict access to this port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-nolisten tcp).

Risk Factor

Low

CVSS Base Score

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

Plugin Information:

Published: 2000/05/12, Modified: 2013/01/25

Plugin Output

tcp/6000

```
X11 Version : 11.0
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/6000

```
Port 6000/tcp was found to be open
```


Synopsis

The remote host is an IRC server.

Description

This plugin determines the version of the IRC daemon.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/11/19, Modified: 2016/01/08

Plugin Output

tcp/6667

```
The IRC server version is : Unreal3.2.8.1. FhiXOoE [*=2309]
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/6667

```
Port 6667/tcp was found to be open
```

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:

Published: 2005/04/06, Modified: 2017/06/08

Plugin Output

tcp/6667

```
An IRC daemon is listening on this port.
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/8009

```
Port 8009/tcp was found to be open
```

Synopsis

There is an AJP connector listening on the remote host.

Description

The remote host is running an AJP (Apache JServ Protocol) connector, a service by which a standalone web server such as Apache communicates over TCP with a Java servlet container such as Tomcat.

See Also

<http://tomcat.apache.org/connectors-doc/>

<http://tomcat.apache.org/connectors-doc/ajp/ajpv13a.html>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/04/05, Modified: 2011/03/11

Plugin Output

tcp/8009

The connector listing on this port supports the ajp13 protocol.

34460 - Unsupported Web Server Detection

Synopsis

The remote web server is obsolete / unsupported.

Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Remove the service if it is no longer needed. Otherwise, upgrade to a newer version if possible or switch to another server.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2008/10/21, Modified: 2018/04/11

Plugin Output

tcp/8180

```
Product      : Tomcat
Installed version : 5.5
Support ended   : 2012-09-30
Supported versions : 8.5.x / 8.0.x / 7.0.x
Additional information : http://tomcat.apache.org/tomcat-55-eol.html
```

Synopsis

The remote web server contains default files.

Description

The default error page, default index page, example JSPs, and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

See Also

<https://wiki.apache.org/tomcat/FAQ/Miscellaneous#Q6>

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

Solution

Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751

XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information:

Published: 2004/03/02, Modified: 2018/01/30

Plugin Output

tcp/8180

The following default files were found :

/tomcat-docs/index.html
/nessus-check/default-404-error-page.html

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:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/8180

```
The remote web server type is :  
Apache-Coyote/1.1
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/8180

```
Port 8180/tcp was found to be open
```

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:

Published: 2003/03/20, Modified: 2018/05/23

Plugin Output

tcp/8180

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

Synopsis

The remote web server contains a graphic image that is prone to information disclosure.

Description

The 'favicon.ico' file found on the remote web server belongs to a popular web server. This may be used to fingerprint the web server.

Solution

Remove the 'favicon.ico' file or create a custom one for your site.

Risk Factor

None

References

XREF OSVDB:39272

Plugin Information:

Published: 2005/10/28, Modified: 2014/10/14

Plugin Output

tcp/8180

```
MD5 fingerprint : 4644f2d45601037b8423d45e13194c93
Web server      : Apache Tomcat or Alfresco Community
```

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/8180

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

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:

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/8180

```
Response Code : HTTP/1.1 200 OK
```

```
Protocol version : HTTP/1.1
```

```
SSL : no
```

```
Keep-Alive : no
```

```
Options allowed : GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
```

```
Headers :
```

```
    Server: Apache-Coyote/1.1
```

```
    Content-Type: text/html; charset=ISO-8859-1
```

```
    Date: Tue, 19 Jun 2018 09:14:24 GMT
```

```
    Connection: close
```

```
Response Body :
```

```
<!--
```

```
Licensed to the Apache Software Foundation (ASF) under one or more  
contributor license agreements. See the NOTICE file distributed with  
this work for additional information regarding copyright ownership.  
The ASF licenses this file to You under the Apache License, Version 2.0  
(the "License"); you may not use this file except in compliance with  
the License. You may obtain a copy of the License at
```

```
    http://www.apache.org/licenses/LICENSE-2.0
```

```
Unless required by applicable law or agreed to in writing, software  
distributed under the License is distributed on an "AS IS" BASIS,
```

WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

```
-->
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
  <head>
    <title>Apache Tomcat/5.5</title>
    <style type="text/css">
      /**/
        body {
          color: #000000;
          background-color: #FFFFFF;
          font-family: Arial, "Times New Roman", Times, serif;
          margin: 10px 0px;
        }

        img {
          border: none;
        }

        a:link, a:visited {
          color: blue
        }

        th {
          font-family: Verdana, "Times New Roman", Times, serif;
          font-size: 110%;
          font-weight: normal;
          font-style: italic;
          background: #D2A41C;
          text-align: left;
        }

        td {
          color: #000000;
          font-family: Arial, Helvetica, sans-serif;
        }

        td.menu {
          background: #FFDC75;
        }

        .center [...]</pre></div><div data-bbox="87 937 177 951" data-label="Page-Footer"><p>192.168.17.21</p></div><div data-bbox="877 937 910 951" data-label="Page-Footer"><p>223</p></div>
```

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

See Also

<https://tomcat.apache.org/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/06/18, Modified: 2018/01/24

Plugin Output

tcp/8180

```
URL      : http://192.168.17.21:8180/  
Version  : 5.5  
backported : 0  
source    : <title>Apache Tomcat/5.5
```


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:

Published: 2002/11/18, Modified: 2016/03/24

Plugin Output

tcp/8787

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      : 8787
Type      : get_http
Banner    :
0x0000:  00 00 00 03 04 08 46 00 00 03 A1 04 08 6F 3A 16      .....F.....O:.
0x0010:  44 52 62 3A 3A 44 52 62 43 6F 6E 6E 45 72 72 6F      DRb::DRbConnErro
0x0020:  72 07 3A 07 62 74 5B 17 22 2F 2F 75 73 72 2F 6C      r.:.bt["./usr/l
0x0030:  69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F      ib/ruby/1.8/drb/
0x0040:  64 72 62 2E 72 62 3A 35 37 33 3A 69 6E 20 60 6C      drb.rb:573:in `l
0x0050:  6F 61 64 27 22 37 2F 75 73 72 2F 6C 69 62 2F 72      oad'"7/usr/lib/r
0x0060:  75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62 2E      uby/1.8/drb/drb.
0x0070:  72 62 3A 36 31 32 3A 69 6E 20 60 72 65 63 76 5F      rb:612:in `recv_
0x0080:  72 65 71 75 65 73 74 27 22 37 2F 75 73 72 2F 6C      request'"7/usr/l
0x0090:  69 62 2F 72 75 62 79 2F 31 2E 38 2F 64 72 62 2F      ib/ruby/1.8/drb/
0x00A0:  64 72 62 2E 72 62 3A 39 31 31 3A 69 6E 20 60 72      drb.rb:911:in `r
0x00B0:  65 63 76 5F 72 65 71 75 65 73 74 27 22 3C 2F 75      ecv_request'"</u
0x00C0:  73 72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F      sr/lib/ruby/1.8/
0x00D0:  64 72 62 2F 64 72 62 2E 72 62 3A 31 35 33 30 3A      drb/drb.rb:1530:
0x00E0:  69 6E 20 60 69 6E 69 74 5F 77 69 74 68 5F 63 6C      in `init_with_cl
0x00F0:  69 65 6E 74 27 22 39 2F 75 73 72 2F 6C 69 62 2F      ient'"9/usr/lib/
0x0100:  72 75 62 79 2F 31 2E 38 2F 64 72 62 2F 64 72 62      ruby/1.8/drb/drb
0x0110:  2E 72 62 3A 31 35 34 32 3A 69 6E 20 60 73 65 74      .rb:1542:in `set
0x0120:  75 70 5F 6D 65 73 73 61 67 65 27 22 33 2F 75 73      up_message'"3/us
0x0130:  72 2F 6C 69 62 2F 72 75 62 79 2F 31 2E 38 2F 64      r/lib/ruby/1.8/d
0x0140:  72 62 2F 64 72 62 2E 72 62 3A 31 34 39 34  [...]  [...]
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/8787

```
Port 8787/tcp was found to be open
```

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/33993

```
The following RPC services are available on UDP port 33993 :
```

- program: 100005 (mountd), version: 1
- program: 100005 (mountd), version: 2
- program: 100005 (mountd), version: 3

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/37007

```
The following RPC services are available on UDP port 37007 :
```

- program: 100021 (nlockmgr), version: 1
- program: 100021 (nlockmgr), version: 3
- program: 100021 (nlockmgr), version: 4

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/40566

```
The following RPC services are available on UDP port 40566 :  
- program: 100024 (status), version: 1
```

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/42278

```
The following RPC services are available on TCP port 42278 :  
- program: 100024 (status), version: 1
```

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/50766

```
The following RPC services are available on TCP port 50766 :
```

- program: 100021 (nlockmgr), version: 1
- program: 100021 (nlockmgr), version: 3
- program: 100021 (nlockmgr), version: 4

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC 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.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/58590

```
The following RPC services are available on TCP port 58590 :
```

- program: 100005 (mountd), version: 1
- program: 100005 (mountd), version: 2
- program: 100005 (mountd), version: 3

192.168.17.31

4

CRITICAL

1

HIGH

5

MEDIUM

2

LOW

49

INFO

Scan Information

Start time: Tue Jun 19 10:41:58 2018

End time: Tue Jun 19 10:46:54 2018

Host Information

Netbios Name: TST-WXP-BUILD26

IP: 192.168.17.31

MAC Address: 00:50:56:b5:47:fc

OS: Microsoft Windows XP Service Pack 2, Microsoft Windows XP Service Pack 3, Windows XP for Embedded Systems

Vulnerabilities

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:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

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 -3 seconds.
```

Synopsis

The remote operating system is no longer supported.

Description

The remote host is running Microsoft Windows XP. Support for this operating system by Microsoft ended April 8th, 2014.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.

See Also

<http://www.nessus.org/u?33ca6af0>

<http://www.nessus.org/u?321523eb>

<https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>

<http://www.nessus.org/u?8dcab5e4>

Solution

Upgrade to a version of Windows that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.2 (CVSS:3.0/E:F/RL:O/RC:X)

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

XREF OSVDB:155633
XREF EDB-ID:41929

Plugin Information:

Published: 2014/03/25, Modified: 2018/01/30

Plugin Output

tcp/0

Synopsis

The remote OS or service pack is no longer supported.

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

See Also

<https://support.microsoft.com/en-us/lifecycle>

Solution

Upgrade to a supported service pack or operating system

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)

Plugin Information:

Published: 2018/04/03, Modified: 2018/04/03

Plugin Output

tcp/0

The following Windows version is installed and not supported:

Microsoft Windows XP Service Pack 2
Microsoft Windows XP Service Pack 3
Windows XP for Embedded Systems

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:

Published: 2003/12/09, Modified: 2018/04/19

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows XP Service Pack 2
Microsoft Windows XP Service Pack 3
Windows XP for Embedded Systems
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.

```
RDP:000000000f00000010000100080001000900000001001000100010
NTP:!:unknown
SMTP:220 tst-wxp-build26 Microsoft ESMTP MAIL Service, Version: 6.0.2600.5949 ready at Tue, 19 Jun
2018 10:42:21 +0200
HTTP:Server: Microsoft-IIS/5.1
```

```
SinFP:
P1:B11113:F0x12:W64240:00204ffff:M1460:
P2:B11113:F0x12:W64240:00204ffff010303000101080a00000000000000001010402:M1460:
P3:B00000:F0x00:W0:00:M0
P4:70101_7_p=1025R
```

```
The remote host is running one of these operating systems :
Microsoft Windows XP Service Pack 2
Microsoft Windows XP Service Pack 3
```


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:

Published: 2005/08/26, Modified: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :  
  
Nessus version : 7.1.1  
Plugin feed version : 201806151820  
Scanner edition used : Nessus  
Scan type : Normal  
Scan policy used : Basic Network Scan  
Scanner IP : 192.168.1.235  
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 : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2018/6/19 10:41 CEST
Scan duration : 296 sec
```

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information:

Published: 2005/10/27, Modified: 2015/10/16

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

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:

Published: 2007/03/12, Modified: 2013/01/07

Plugin Output

tcp/0

```
It was not possible to connect to '\\TST-WXP-BUILD26\ADMIN$' with the supplied credentials.
```

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:

Published: 2007/05/16, Modified: 2011/03/20

Plugin Output

tcp/0

Synopsis

The remote IP address seems to connect to different hosts via reverse NAT, or an intercepting proxy is in the way.

Description

Reverse NAT is a technology which lets multiple computers offer public services on different ports via the same IP address.

Based on OS fingerprinting results, it seems that different operating systems are listening on different remote ports.

Note that this behavior may also indicate the presence of a intercepting proxy, a load balancer or a traffic shaper.

See Also

https://en.wikipedia.org/wiki/Proxy_server#Intercepting_proxy_server

Solution

Make sure that this setup is authorized by your security policy

Risk Factor

None

Plugin Information:

Published: 2008/03/12, Modified: 2017/06/12

Plugin Output

tcp/0

```
+ On the following port(s) :  
- 80 (0 hops away)  
  
The operating system was identified as :  
  
pfSense  
  
+ On the following port(s) :  
- 135 (1 hops away)  
- 3389 (1 hops away)  
- 445 (1 hops away)  
- 139 (1 hops away)  
- 21 (1 hops away)  
- 25 (1 hops away)  
- 1025 (1 hops away)  
- 443 (1 hops away)
```

The operating system was identified as :

EMC CLARiION AX150SCi SAN Disk Array

EMC CLARiION CX3-10 SAN Disk Array

Microsoft Windows 2000

Microsoft Windows XP

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:

Published: 2009/02/19, Modified: 2017/11/17

Plugin Output

tcp/0

```
The following card manufacturers were identified :
```

```
00:50:56:b5:47:fc : VMware, Inc.
```


45590 - Common Platform Enumeration (CPE)

Synopsis

It was 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/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/04/21, Modified: 2017/06/06

Plugin Output

tcp/0

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

```
cpe:/o:microsoft:windows_xp::sp2 -> Microsoft Windows XP Service Pack 2
cpe:/o:microsoft:windows_xp::sp3 -> Microsoft Windows XP Service Pack 3
cpe:/o:microsoft:windows
```

```
Following application CPE matched on the remote system :
```

```
cpe:/a:microsoft:iis:5.1 -> Microsoft IIS 5.1
```

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:

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 99
```

108804 - Microsoft Exchange Server Detection (Uncredentialed)

Synopsis

The remote host is running an Exchange Server.

Description

One or more Microsoft Exchange servers are listening on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/04/03, Modified: 2018/04/03

Plugin Output

tcp/0

```
Path      :  
Version   : unknown
```

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/11/27, Modified: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.235 to 192.168.17.31 :
192.168.1.235
192.168.7.252
192.168.17.31

Hop Count: 2
```

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:

Published: 1999/10/12, Modified: 2018/02/12

Plugin Output

tcp/21

```
The remote FTP banner is :  
220 Microsoft FTP Service
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/21

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

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/21

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

54582 - SMTP Service Cleartext Login Permitted

Synopsis

The remote mail server allows cleartext logins.

Description

The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used.

See Also

<https://tools.ietf.org/html/rfc4422>

<https://tools.ietf.org/html/rfc4954>

Solution

Configure the service to support less secure authentication mechanisms only over an encrypted channel.

Risk Factor

Low

CVSS Base Score

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

Plugin Information:

Published: 2011/05/19, Modified: 2017/06/12

Plugin Output

tcp/25

```
The SMTP server advertises the following SASL methods over an
unencrypted channel :
```

```
  All supported methods : NTLM, LOGIN, GSSAPI
  Cleartext methods      : LOGIN
```


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:

Published: 1999/10/12, Modified: 2011/03/11

Plugin Output

tcp/25

Remote SMTP server banner :

```
220 tst-wxp-build26 Microsoft ESMTP MAIL Service, Version: 6.0.2600.5949 ready at Tue, 19 Jun 2018
10:42:21 +0200
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/25

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

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/25

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

Synopsis

The remote mail server supports authentication.

Description

The remote SMTP server advertises that it supports authentication.

See Also

<https://tools.ietf.org/html/rfc4422>

<https://tools.ietf.org/html/rfc4954>

Solution

Review the list of methods and whether they're available over an encrypted channel.

Risk Factor

None

Plugin Information:

Published: 2011/05/19, Modified: 2018/03/28

Plugin Output

tcp/25

```
The following authentication methods are advertised by the SMTP
server without encryption :
  GSSAPI
  LOGIN
  NTLM
```

Synopsis

Nessus can obtain information about the host by examining the NTLM SSP message.

Description

Nessus can obtain information about the host by examining the NTLM SSP challenge issued during NTLM authentication, over SMTP.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/03/28, Modified: 2018/03/28

Plugin Output

tcp/25

Nessus was able to obtain the following information about the host, by parsing the SMTP server's NTLM SSP message:

Target Name:	TST-WXP-BUILD26
NetBIOS Domain Name:	TST-WXP-BUILD26
NetBIOS Computer Name:	TST-WXP-BUILD26
DNS Domain Name:	tst-wxp-build26
DNS Computer Name:	tst-wxp-build26
DNS Tree Name:	unknown
Product Version:	5.1.2600

97994 - Microsoft IIS 6.0 Unsupported Version Detection

Synopsis

An unsupported version of Microsoft IIS is running on the remote Windows host.

Description

According to its self-reported version number, the installation of Microsoft Internet Information Services (IIS) 6.0 on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

<http://www.nessus.org/u?d99a8431>

<https://www.microsoft.com/en-us/cloud-platform/windows-server-2003>

Solution

Upgrade to a version of Microsoft IIS that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2017/04/17, Modified: 2017/04/17

Plugin Output

tcp/80

```
Installed version : 5.1
Supported versions : 7.0 or later
EOL date         : 2015/07/14
EOL URL          : http://www.nessus.org/u?d99a8431
```

34460 - Unsupported Web Server Detection

Synopsis

The remote web server is obsolete / unsupported.

Description

According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Remove the service if it is no longer needed. Otherwise, upgrade to a newer version if possible or switch to another server.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2008/10/21, Modified: 2018/04/11

Plugin Output

tcp/80

```
Product           : Microsoft IIS 5.1
Server response header : Microsoft-IIS/5.1
Support ended      : 2014-04-08
Supported versions  : Microsoft IIS 8.5 / 8.0 / 7.5 / 7.0
Additional information : http://support.microsoft.com/lifecycle/?p1=2096
```

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:

Published: 2003/01/23, Modified: 2018/05/21

Plugin Output

tcp/80

Use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy.

Nessus sent the following TRACE request :

```
----- snip -----
TRACE /Nessus1099094729.html HTTP/1.1
Connection: Close
Host: 192.168.17.31
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
Server: Microsoft-IIS/5.1
Date: Tue, 19 Jun 2018 08:45:59 GMT
X-Powered-By: ASP.NET
Content-Type: message/http
Content-Length: 378
X-Cache: MISS from localhost
X-Cache-Lookup: NONE from localhost:3128
Connection: keep-alive
```

```
TRACE /Nessus1099094729.html HTTP/1.1
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
Host: 192.168.17.31
X-Forwarded-For: 192.168.1.235
Cache-Control: max-age=259200
Connection: keep-alive
```

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

Synopsis

FrontPage extensions are enabled.

Description

The remote web server appears to be running with the FrontPage extensions.

FrontPage allows remote web developers and administrators to modify web content from a remote location. While this is a fairly typical scenario on an internal local area network, the FrontPage extensions should not be available to anonymous users via the Internet (or any other untrusted 3rd party network).

Solution

n/a

Risk Factor

None

References

CVE	CVE-2000-0114
XREF	OSVDB:67

Plugin Information:

Published: 1999/08/22, Modified: 2014/06/09

Plugin Output

tcp/80

```
The remote frontpage server leaks information regarding the name of the anonymous user.  
By knowing the name of the anonymous user, more sophisticated attacks may be launched.  
We could gather that the name of the anonymous user is : IUSR_TST-WXP-BUILD26
```

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:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/80

```
The remote web server type is :  
Microsoft-IIS/5.1
```

Synopsis

Indexing Service filter is enabled on the remote Web server.

Description

The IIS server appears to have the .IDA ISAPI filter mapped.

At least one remote vulnerability has been discovered for the .IDA (indexing service) filter. This is detailed in Microsoft Advisory MS01-033, and gives remote SYSTEM level access to the web server.

It is recommended that even if you have patched this vulnerability that you unmap the .IDA extension, and any other unused ISAPI extensions if they are not required for the operation of your site.

Solution

To unmap the .IDA extension:

1.Open Internet Services Manager. 2.Right-click the Web server choose Properties from the context menu. 3.Master Properties 4.Select WWW Service -> Edit -> HomeDirectory -> Configuration 5.Remove the reference to .ida from the list.

In addition, you may wish to download and install URLSCAN from the Microsoft Technet website. URLSCAN, by default, blocks all .ida requests to the IIS server.

Risk Factor

None

Plugin Information:

Published: 2001/06/19, Modified: 2014/04/25

Plugin Output

tcp/80

Synopsis

A transparent or reverse HTTP proxy is running on this port.

Description

This web server is reachable through a reverse HTTP proxy.

Solution

n/a

Risk Factor

None

References

CVE	CVE-2004-2320
CVE	CVE-2005-3398
CVE	CVE-2005-3498
CVE	CVE-2007-3008
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:35511
XREF	OSVDB:50485
XREF	CWE:200
XREF	CWE:79

Plugin Information:

Published: 2002/07/02, Modified: 2018/05/21

Plugin Output

tcp/80

```
There might be a caching proxy on the way to this web server:
MISS from localhost
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/80

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

Synopsis

The remote web server is running Microsoft IIS.

Description

The Patch level (Service Pack) of the remote IIS server appears to be lower than the current IIS service pack level. As each service pack typically contains many security patches, the server may be at risk.

Note that this test makes assumptions of the remote patch level based on static return values (Content-Length) within a IIS Server's 404 error message. As such, the test can not be totally reliable and should be manually confirmed.

Note also that, to determine IIS6 patch levels, a simple test is done based on strict RFC 2616 compliance. It appears as if IIS6-SP1 will accept CR as an end-of-line marker instead of both CR and LF.

Solution

Ensure that the server is running the latest stable Service Pack.

Risk Factor

None

Plugin Information:

Published: 2003/10/09, Modified: 2011/06/01

Plugin Output

tcp/80

```
The remote IIS server *seems* to be Microsoft IIS 5.1 - SP0
```

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/80

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


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:

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/80

```
Response Code : HTTP/1.1 200 OK
```

```
Protocol version : HTTP/1.1
```

```
SSL : no
```

```
Keep-Alive : no
```

```
Options allowed : (Not implemented)
```

```
Headers :
```

```
    Server: Microsoft-IIS/5.1
```

```
    Date: Tue, 19 Jun 2018 08:45:58 GMT
```

```
    X-Powered-By: ASP.NET
```

```
    Content-Length: 1330
```

```
    Content-Type: text/html
```

```
    Cache-Control: private
```

```
    X-Cache: MISS from localhost
```

```
    X-Cache-Lookup: MISS from localhost:3128
```

```
    Connection: keep-alive
```

```
Response Body :
```

```
<!--
```

```
    WARNING!
```

```
    Please do not alter this file. It may be replaced if you upgrade your web server
```

```
    If you want to use it as a template, we recommend renaming it, and modifying the new file.
```

```
    Thanks.
```

```
-->

<html>

<head>
<meta HTTP-EQUIV="Content-Type" Content="text-html; charset=Windows-1252">

<title id=titletext>Under Construction</title>
</head>

  <body bgcolor=white>
    <table>
      <tr>
        <td id="tableProps" width=70 valign=top align=center>
          
        <td id="tablePropsWidth" width=400>

          <h1 id=errortype style="font:14pt/16pt verdana; color:#4e4e4e">
            <id id="Comment1"><!--Problem--></id><id id="errorText">Under Construction</id></h1>
            <id id="Comment2"><!--Probable causes:--></id><id id="errordesc"><font style="font:9pt/12pt
            verdana; color:black">
              The site you were trying to reach does not currently have a default page. It may be in the process
              of being upgraded and configured.
            </id>
            <br><br>

            <hr size=1 color="blue">

            <br>
            <id id=term1>
              Please try this site again later. If you still experience the problem, try contacting the Web site
              administrator.
            </id>
            <p>

          </ul>
          <br>
        </td>
      </tr>
    </table>
  </body>

</html>
```

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:

Published: 2009/12/10, Modified: 2018/06/11

Plugin Output

tcp/80

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

```
- HTTP methods COPY GET HEAD LOCK PROPFIND SEARCH TRACE  
  UNLOCK OPTIONS are allowed on :
```

```
/
```

Synopsis

An NTP server is listening on the remote host.

Description

An NTP server is listening on port 123. If not securely configured, it may provide information about its version, current date, current time, and possibly system information.

See Also

<http://www.ntp.org>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2015/03/20, Modified: 2018/05/07

Plugin Output

udp/123

```
An NTP service has been discovered, listening on port 123.
```

```
No sensitive information has been disclosed.
```

```
Version : unknown
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/135

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

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:

Published: 1999/10/12, Modified: 2018/06/06

Plugin Output

udp/137

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

```
TST-WXP-BUILD26  = Computer name
WORKGROUP        = Workgroup / Domain name
TST-WXP-BUILD26  = File Server Service
WORKGROUP        = Browser Service Elections
WORKGROUP        = Master Browser
__MSBROWSE__     = Master Browser
```

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

```
00:50:56:b5:47:fc
```

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:

Published: 2002/06/05, Modified: 2015/06/02

Plugin Output

tcp/139

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

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/139

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


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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/443

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

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled. It is, therefore, affected by multiple vulnerabilities :

- Multiple information disclosure vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to disclose sensitive information. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276)
- Multiple denial of service vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMB request, to cause the system to stop responding. (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280)
- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to execute arbitrary code. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279)

Depending on the host's security policy configuration, this plugin cannot always correctly determine if the Windows host is vulnerable if the host is running a later Windows version (i.e., Windows 8.1, 10, 2012, 2012 R2, and 2016) specifically that named pipes and shares are allowed to be accessed remotely and anonymously. Tenable does not recommend this configuration, and the hosts should be checked locally for patches with one of the following plugins, depending on the Windows version : 100054, 100055, 100057, 100059, 100060, or 100061.

See Also

<http://www.nessus.org/u?c21268d4>
<http://www.nessus.org/u?b9253982>
<http://www.nessus.org/u?23802c83>
<http://www.nessus.org/u?8313bb60>
<http://www.nessus.org/u?7677c678>
<http://www.nessus.org/u?36da236c>
<http://www.nessus.org/u?0981b934>
<http://www.nessus.org/u?c88efefa>
<http://www.nessus.org/u?695bf5cc>
<http://www.nessus.org/u?459a1e8c>
<http://www.nessus.org/u?ea45bbc5>
<http://www.nessus.org/u?4195776a>
<http://www.nessus.org/u?fbf092cf>

Solution

Apply the applicable security update for your Windows version :

- Windows Server 2008 : KB4018466
- Windows 7 : KB4019264
- Windows Server 2008 R2 : KB4019264
- Windows Server 2012 : KB4019216
- Windows 8.1 / RT 8.1. : KB4019215
- Windows Server 2012 R2 : KB4019215
- Windows 10 : KB4019474
- Windows 10 Version 1511 : KB4019473
- Windows 10 Version 1607 : KB4019472
- Windows 10 Version 1703 : KB4016871
- Windows Server 2016 : KB4019472

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 v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

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

CVSS Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

BID	98259
BID	98260
BID	98261
BID	98263
BID	98264
BID	98265

BID	98266
BID	98267
BID	98268
BID	98270
BID	98271
BID	98272
BID	98273
BID	98274
CVE	CVE-2017-0267
CVE	CVE-2017-0268
CVE	CVE-2017-0269
CVE	CVE-2017-0270
CVE	CVE-2017-0271
CVE	CVE-2017-0272
CVE	CVE-2017-0273
CVE	CVE-2017-0274
CVE	CVE-2017-0275
CVE	CVE-2017-0276
CVE	CVE-2017-0277
CVE	CVE-2017-0278
CVE	CVE-2017-0279
CVE	CVE-2017-0280
MSKB	4016871
MSKB	4018466
MSKB	4019213
MSKB	4019214
MSKB	4019215
MSKB	4019216
MSKB	4019263
MSKB	4019264
MSKB	4019472
MSKB	4019473
MSKB	4019474
XREF	OSVDB:157230
XREF	OSVDB:157231
XREF	OSVDB:157232
XREF	OSVDB:157233
XREF	OSVDB:157234
XREF	OSVDB:157235
XREF	OSVDB:157236
XREF	OSVDB:157237
XREF	OSVDB:157238
XREF	OSVDB:157239

XREF	OSVDB:157240
XREF	OSVDB:157246
XREF	OSVDB:157247
XREF	OSVDB:157248

Plugin Information:

Published: 2017/05/26, Modified: 2017/08/15

Plugin Output

tcp/445

Synopsis

It is possible to log into the remote Windows host with a NULL session.

Description

The remote host is running Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password).

Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.

See Also

<http://support.microsoft.com/kb/q143474/>

<http://support.microsoft.com/kb/q246261/>

[http://technet.microsoft.com/en-us/library/cc785969\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx)

Solution

Apply the following registry changes per the referenced Technet advisories :

Set :

- HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1

Remove BROWSER from :

- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes

Reboot once the registry changes are complete.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.2 (CVSS2#E:U/RL:U/RC:ND)

References

BID 494

CVE	CVE-1999-0519
CVE	CVE-1999-0520
CVE	CVE-2002-1117
XREF	OSVDB:299
XREF	OSVDB:8230

Plugin Information:

Published: 2007/10/04, Modified: 2012/02/29

Plugin Output

tcp/445

```
It was possible to bind to the \browser pipe
```

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 v3.0 Base Score

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

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

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:

Published: 2012/01/19, Modified: 2018/05/02

Plugin Output

tcp/445

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

<https://support.microsoft.com/kb/143474>

<https://support.microsoft.com/kb/246261>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/05/09, Modified: 2018/06/06

Plugin Output

tcp/445

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

Synopsis

It is possible to obtain network information.

Description

It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Solution

n/a

Risk Factor

None

References

XREF OSVDB:300

Plugin Information:

Published: 2000/05/09, Modified: 2015/01/12

Plugin Output

tcp/445

```
Here is the browse list of the remote host :
```

```
DESKTOP-1PS9M10 ( os : 10.0 )  
METASPLOITABLE ( os : 4.9 ) -  
SAGS-FXWV1C5WK5 ( os : 5.2 )  
TST-WXP-BUILD26 ( os : 5.1 )
```

Synopsis

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

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/10/17, Modified: 2017/11/30

Plugin Output

tcp/445

```
The remote Operating System is : Windows 5.1
The remote native LAN manager is : Windows 2000 LAN Manager
The remote SMB Domain Name is : TST-WXP-BUILD26
```

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:

Published: 2002/06/05, Modified: 2015/06/02

Plugin Output

tcp/445

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

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/445

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

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:

Published: 2007/10/04, Modified: 2011/03/27

Plugin Output

tcp/445

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

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

<https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>

<https://support.microsoft.com/en-us/kb/2696547>

<http://www.nessus.org/u?8dcab5e4>

<http://www.nessus.org/u?36fd3072>

<http://www.nessus.org/u?4c7e0cf3>

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF OSVDB:151058

Plugin Information:

Published: 2017/02/03, Modified: 2017/02/16

Plugin Output

tcp/445

```
The remote host supports SMBv1.
```


Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2017/06/19, Modified: 2017/06/19

Plugin Output

tcp/445

```
The remote host supports the following versions of SMB :  
SMBv1
```

Synopsis

It was possible to obtain information about the dialects of SMB2 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/02/09, Modified: 2018/02/09

Plugin Output

tcp/445

```
The remote host does NOT support the following SMB dialects :
 _version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.0        Windows 8
3.0.2      Windows 8.1
3.1        Windows 10
3.1.1      Windows 10
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/1025

```
Port 1025/tcp was found to be open
```

Synopsis

A DCE/RPC server is listening on the remote host.

Description

The remote host is running a Windows RPC service. This service replies to the RPC Bind Request with a Bind Ack response.

However it is not possible to determine the uuid of this service.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/09/11, Modified: 2011/03/11

Plugin Output

tcp/1025

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?8033da0d>

<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:

Published: 2005/06/01, Modified: 2018/05/10

Plugin Output

tcp/3389

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:

Published: 2012/01/25, Modified: 2018/05/16

Plugin Output

tcp/3389

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

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:

Published: 2008/02/11, Modified: 2018/05/16

Plugin Output

tcp/3389

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


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:

Published: 2002/04/20, Modified: 2017/08/07

Plugin Output

tcp/3389

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/3389

```
Port 3389/tcp was found to be open
```

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:

Published: 2013/04/22, Modified: 2018/05/21

Plugin Output

tcp/3389

```
It was possible to gather the following screenshot of the remote login screen.
```


192.168.17.41

3

CRITICAL

0

HIGH

5

MEDIUM

1

LOW

40

INFO

Scan Information

Start time: Tue Jun 19 10:48:37 2018

End time: Tue Jun 19 10:52:22 2018

Host Information

Netbios Name: SAGS-FXWV1C5WK5

IP: 192.168.17.41

MAC Address: 00:50:56:b5:02:00

OS: Microsoft Windows Server 2003 Service Pack 2

Vulnerabilities

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:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

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 -2 seconds.
```

Synopsis

The remote operating system is no longer supported.

Description

The remote host is running Microsoft Windows Server 2003. Support for this operating system by Microsoft ended July 14th, 2015.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.

See Also

<http://www.nessus.org/u?c0dbe792>

<http://www.nessus.org/u?321523eb>

<https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>

<http://www.nessus.org/u?8dcab5e4>

Solution

Upgrade to a version of Windows that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.2 (CVSS:3.0/E:F/RL:O/RC:X)

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

XREF	OSVDB:155633
XREF	EDB-ID:41929

Plugin Information:

Published: 2015/07/14, Modified: 2017/11/21

Plugin Output

tcp/0

Synopsis

The remote OS or service pack is no longer supported.

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

See Also

<https://support.microsoft.com/en-us/lifecycle>

Solution

Upgrade to a supported service pack or operating system

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)

Plugin Information:

Published: 2018/04/03, Modified: 2018/04/03

Plugin Output

tcp/0

```
The following Windows version is installed and not supported:  
Microsoft Windows Server 2003 Service Pack 2
```

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:

Published: 2003/12/09, Modified: 2018/04/19

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows Server 2003 Service Pack 2
Confidence level : 99
Method : MSRPC
```

```
The remote host is running Microsoft Windows Server 2003 Service Pack 2
```

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:

Published: 2005/08/26, Modified: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :  
  
Nessus version : 7.1.1  
Plugin feed version : 201806151820  
Scanner edition used : Nessus  
Scan type : Normal  
Scan policy used : Basic Network Scan  
Scanner IP : 192.168.1.235  
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 : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2018/6/19 10:48 CEST
Scan duration : 224 sec
```

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information:

Published: 2005/10/27, Modified: 2015/10/16

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

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:

Published: 2007/03/12, Modified: 2013/01/07

Plugin Output

tcp/0

```
It was not possible to connect to '\\SAGS-FXWV1C5WK5\ADMIN$' with the supplied credentials.
```

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:

Published: 2007/05/16, Modified: 2011/03/20

Plugin Output

tcp/0

Synopsis

The remote IP address seems to connect to different hosts via reverse NAT, or an intercepting proxy is in the way.

Description

Reverse NAT is a technology which lets multiple computers offer public services on different ports via the same IP address.

Based on OS fingerprinting results, it seems that different operating systems are listening on different remote ports.

Note that this behavior may also indicate the presence of a intercepting proxy, a load balancer or a traffic shaper.

See Also

https://en.wikipedia.org/wiki/Proxy_server#Intercepting_proxy_server

Solution

Make sure that this setup is authorized by your security policy

Risk Factor

None

Plugin Information:

Published: 2008/03/12, Modified: 2017/06/12

Plugin Output

tcp/0

```
+ On the following port(s) :  
- 80 (0 hops away)  
  
The operating system was identified as :  
  
pfSense  
  
+ On the following port(s) :  
- 135 (1 hops away)  
- 3389 (1 hops away)  
- 445 (1 hops away)  
- 139 (1 hops away)  
- 2994 (1 hops away)  
- 21 (1 hops away)  
- 1026 (1 hops away)  
- 1025 (1 hops away)
```


The operating system was identified as :

Microsoft Windows Server 2003

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:

Published: 2009/02/19, Modified: 2017/11/17

Plugin Output

tcp/0

```
The following card manufacturers were identified :
```

```
00:50:56:b5:02:00 : VMware, Inc.
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was 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/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/04/21, Modified: 2017/06/06

Plugin Output

tcp/0

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

```
cpe:/o:microsoft:windows_2003_server::sp2 -> Microsoft Windows 2003 Server Service Pack 2
```

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:

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 99
```

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/11/27, Modified: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.235 to 192.168.17.41 :
192.168.1.235
192.168.7.252
192.168.17.41

Hop Count: 2
```

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:

Published: 1999/10/12, Modified: 2018/02/12

Plugin Output

tcp/21

```
The remote FTP banner is :  
220 Microsoft FTP Service
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/21

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

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/21

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


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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/80

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

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/80

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

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:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

tcp/135

The following DCERPC services are available locally :

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 : Local RPC service
Named pipe : dhcpcsvc

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 : Local RPC service
Named pipe : DNSResolver

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fblcdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE910A74AB1AB14F23899AB6F46044

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fblcdd53, version 1.0
Description : Scheduler Service

Windows process : svchost.exe
Type : Local RPC service
Named pipe : wzcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE910A74AB1AB14F23899AB6F46044

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : wzcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE910A74AB1AB14F23899AB6F46044

Object UUID : 82bb9077-64a8-11e8-9047-005056b50200
UUID : f1ec59ab-4ca9-4c30-b2d0-54ef1db441b7, version 1.0
Description : Unknown RPC service
Annotation : Isolation Communication Endpoint
Type : Local RPC service
Named pipe : LRPC000008c8.00000001

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-c [...]

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/135

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

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:

Published: 1999/10/12, Modified: 2018/06/06

Plugin Output

udp/137

```
The following 4 NetBIOS names have been gathered :
```

```
SAGS-FXWV1C5WK5  = Computer name
WORKGROUP        = Workgroup / Domain name
SAGS-FXWV1C5WK5  = File Server Service
WORKGROUP        = Browser Service Elections
```

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

```
00:50:56:b5:02:00
```

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:

Published: 2002/06/05, Modified: 2015/06/02

Plugin Output

tcp/139

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

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/139

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


Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled. It is, therefore, affected by multiple vulnerabilities :

- Multiple information disclosure vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to disclose sensitive information. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276)
- Multiple denial of service vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMB request, to cause the system to stop responding. (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280)
- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to execute arbitrary code. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279)

Depending on the host's security policy configuration, this plugin cannot always correctly determine if the Windows host is vulnerable if the host is running a later Windows version (i.e., Windows 8.1, 10, 2012, 2012 R2, and 2016) specifically that named pipes and shares are allowed to be accessed remotely and anonymously. Tenable does not recommend this configuration, and the hosts should be checked locally for patches with one of the following plugins, depending on the Windows version : 100054, 100055, 100057, 100059, 100060, or 100061.

See Also

<http://www.nessus.org/u?c21268d4>
<http://www.nessus.org/u?b9253982>
<http://www.nessus.org/u?23802c83>
<http://www.nessus.org/u?8313bb60>
<http://www.nessus.org/u?7677c678>
<http://www.nessus.org/u?36da236c>
<http://www.nessus.org/u?0981b934>
<http://www.nessus.org/u?c88efefa>
<http://www.nessus.org/u?695bf5cc>
<http://www.nessus.org/u?459a1e8c>
<http://www.nessus.org/u?ea45bbc5>
<http://www.nessus.org/u?4195776a>
<http://www.nessus.org/u?fbf092cf>

Solution

Apply the applicable security update for your Windows version :

- Windows Server 2008 : KB4018466
- Windows 7 : KB4019264
- Windows Server 2008 R2 : KB4019264
- Windows Server 2012 : KB4019216
- Windows 8.1 / RT 8.1. : KB4019215
- Windows Server 2012 R2 : KB4019215
- Windows 10 : KB4019474
- Windows 10 Version 1511 : KB4019473
- Windows 10 Version 1607 : KB4019472
- Windows 10 Version 1703 : KB4016871
- Windows Server 2016 : KB4019472

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 v3.0 Temporal Score

8.5 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

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

CVSS Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

BID	98259
BID	98260
BID	98261
BID	98263
BID	98264
BID	98265

BID	98266
BID	98267
BID	98268
BID	98270
BID	98271
BID	98272
BID	98273
BID	98274
CVE	CVE-2017-0267
CVE	CVE-2017-0268
CVE	CVE-2017-0269
CVE	CVE-2017-0270
CVE	CVE-2017-0271
CVE	CVE-2017-0272
CVE	CVE-2017-0273
CVE	CVE-2017-0274
CVE	CVE-2017-0275
CVE	CVE-2017-0276
CVE	CVE-2017-0277
CVE	CVE-2017-0278
CVE	CVE-2017-0279
CVE	CVE-2017-0280
MSKB	4016871
MSKB	4018466
MSKB	4019213
MSKB	4019214
MSKB	4019215
MSKB	4019216
MSKB	4019263
MSKB	4019264
MSKB	4019472
MSKB	4019473
MSKB	4019474
XREF	OSVDB:157230
XREF	OSVDB:157231
XREF	OSVDB:157232
XREF	OSVDB:157233
XREF	OSVDB:157234
XREF	OSVDB:157235
XREF	OSVDB:157236
XREF	OSVDB:157237
XREF	OSVDB:157238
XREF	OSVDB:157239

XREF	OSVDB:157240
XREF	OSVDB:157246
XREF	OSVDB:157247
XREF	OSVDB:157248

Plugin Information:

Published: 2017/05/26, Modified: 2017/08/15

Plugin Output

tcp/445

Synopsis

It is possible to log into the remote Windows host with a NULL session.

Description

The remote host is running Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password).

Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.

See Also

<http://support.microsoft.com/kb/q143474/>

<http://support.microsoft.com/kb/q246261/>

[http://technet.microsoft.com/en-us/library/cc785969\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx)

Solution

Apply the following registry changes per the referenced Technet advisories :

Set :

- HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1

Remove BROWSER from :

- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes

Reboot once the registry changes are complete.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.2 (CVSS2#E:U/RL:U/RC:ND)

References

BID 494

CVE	CVE-1999-0519
CVE	CVE-1999-0520
CVE	CVE-2002-1117
XREF	OSVDB:299
XREF	OSVDB:8230

Plugin Information:

Published: 2007/10/04, Modified: 2012/02/29

Plugin Output

tcp/445

```
It was possible to bind to the \browser pipe
```

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 v3.0 Base Score

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

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

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:

Published: 2012/01/19, Modified: 2018/05/02

Plugin Output

tcp/445

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

<https://support.microsoft.com/kb/143474>

<https://support.microsoft.com/kb/246261>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/05/09, Modified: 2018/06/06

Plugin Output

tcp/445

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

Synopsis

It is possible to obtain network information.

Description

It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Solution

n/a

Risk Factor

None

References

XREF OSVDB:300

Plugin Information:

Published: 2000/05/09, Modified: 2015/01/12

Plugin Output

tcp/445

```
Here is the browse list of the remote host :
```

```
DESKTOP-1PS9M10 ( os : 10.0 )  
METASPLOITABLE ( os : 4.9 ) -  
SAGS-FXWV1C5WK5 ( os : 5.2 )  
TST-WXP-BUILD26 ( os : 5.1 )
```

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:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

tcp/445

The following DCERPC services are available remotely :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fblcdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\SAGS-FXWV1C5WK5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\SAGS-FXWV1C5WK5

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 : \\SAGS-FXWV1C5WK5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2f5f6521-cb55-1059-b446-00df0bce31db, version 1.0

Description : Telephony service
Windows process : svchost.exe
Annotation : Unimodem LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\tapsrv
Netbios name : \\SAGS-FXWV1C5WK5

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 82ad4280-036b-11cf-972c-00aa006887b0, version 2.0
Description : Internet Information Service (IISAdmin)
Windows process : inetinfo.exe
Type : Remote RPC service
Named pipe : \PIPE\INETINFO
Netbios name : \\SAGS-FXWV1C5WK5

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
Named pipe : \PIPE\lsass
Netbios name : \\SAGS-FXWV1C5WK5

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
Named pipe : \PIPE\protected_storage
Netbios name : \\SAGS-FXWV1C5WK5

Object UUID : 000000 [...]

Synopsis

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

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/10/17, Modified: 2017/11/30

Plugin Output

tcp/445

```
The remote Operating System is : Windows Server 2003 3790 Service Pack 2
The remote native LAN manager is : Windows Server 2003 5.2
The remote SMB Domain Name is : SAGS-FXWV1C5WK5
```

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:

Published: 2002/06/05, Modified: 2015/06/02

Plugin Output

tcp/445

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

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/445

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

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:

Published: 2007/10/04, Modified: 2011/03/27

Plugin Output

tcp/445

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


Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

<https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>

<https://support.microsoft.com/en-us/kb/2696547>

<http://www.nessus.org/u?8dcab5e4>

<http://www.nessus.org/u?36fd3072>

<http://www.nessus.org/u?4c7e0cf3>

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF OSVDB:151058

Plugin Information:

Published: 2017/02/03, Modified: 2017/02/16

Plugin Output

tcp/445

```
The remote host supports SMBv1.
```

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2017/06/19, Modified: 2017/06/19

Plugin Output

tcp/445

```
The remote host supports the following versions of SMB :  
SMBv1
```

Synopsis

It was possible to obtain information about the dialects of SMB2 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/02/09, Modified: 2018/02/09

Plugin Output

tcp/445

```
The remote host does NOT support the following SMB dialects :
 _version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.0         Windows 8
3.0.2       Windows 8.1
3.1         Windows 10
3.1.1       Windows 10
```

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
MSKB	3148527
MSKB	3149090

MSKB	3147461
MSKB	3147458
XREF	OSVDB:136339
XREF	MSFT:MS16-047
XREF	CERT:813296
XREF	IAVA:2016-A-0093

Plugin Information:

Published: 2016/04/13, Modified: 2017/08/30

Plugin Output

tcp/1025

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:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

tcp/1025

```
The following DCERPC services are available on TCP port 1025 :
```

```
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 : 1025
IP : 192.168.17.41
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/1025

```
Port 1025/tcp was found to be open
```

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:

Published: 2001/08/26, Modified: 2014/05/12

Plugin Output

tcp/1026

The following DCERPC services are available on TCP port 1026 :

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 82ad4280-036b-11cf-972c-00aa006887b0, version 2.0
Description : Internet Information Service (IISAdmin)
Windows process : inetinfo.exe
Type : Remote RPC service
TCP Port : 1026
IP : 192.168.17.41
```


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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/1026

```
Port 1026/tcp was found to be open
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/2994

```
Port 2994/tcp was found to be open
```

Synopsis

A DCE/RPC server is listening on the remote host.

Description

The remote host is running a Windows RPC service. This service replies to the RPC Bind Request with a Bind Ack response.

However it is not possible to determine the uuid of this service.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/09/11, Modified: 2011/03/11

Plugin Output

tcp/2994

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?8033da0d>

<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:

Published: 2005/06/01, Modified: 2018/05/10

Plugin Output

tcp/3389

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:

Published: 2012/01/25, Modified: 2018/05/16

Plugin Output

tcp/3389

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

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:

Published: 2008/02/11, Modified: 2018/05/16

Plugin Output

tcp/3389

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

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:

Published: 2002/04/20, Modified: 2017/08/07

Plugin Output

tcp/3389

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/3389

```
Port 3389/tcp was found to be open
```

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:

Published: 2013/04/22, Modified: 2018/05/21

Plugin Output

tcp/3389

```
It was possible to gather the following screenshot of the remote login screen.
```


192.168.17.53

2

CRITICAL

1

HIGH

53

MEDIUM

15

LOW

152

INFO

Scan Information

Start time: Tue Jun 19 10:51:53 2018

End time: Tue Jun 19 11:02:24 2018

Host Information

Netbios Name: BEE-BOX

IP: 192.168.17.53

MAC Address: 00:50:56:b5:1a:ad

OS: Linux Kernel 2.6.24-16-generic

Vulnerabilities

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:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -79 seconds.
```

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:

Published: 2003/12/09, Modified: 2018/04/19

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.6.24-16-generic (i386)
Confidence level : 98
Method : NTP

Primary method : SNMP

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.

SSH:SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
mDNS:LINUX
SNMP:Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i686
NTP:Linux/2.6.24-16-generic
SinFP:
  P1:B10113:F0x12:W5840:00204ffff:M1460:
  P2:B10113:F0x12:W5792:00204ffff0402080affffff4445414401030307:M1460:
  P3:B00000:F0x00:W0:00:M0
  P4:70101_7_p=514R
SMTP:!:220 bee-box ESMTP Postfix (Ubuntu)
SSLcert:!:i/CN:bee-box.bwapp.locali/O:MMEi/OU:ITs/CN:bee-box.bwapp.locals/O:MMEs/OU:IT
ae5fb7be864a78e168318fc1c96a4bd242c4e6c3
i/CN:bee-box.bwapp.locali/O:MMEi/OU:ITs/CN:bee-box.bwapp.locals/O:MMEs/OU:IT
ae5fb7be864a78e168318fc1c96a4bd242c4e6c3
i/CN:bee-box.bwapp.locali/O:MMEi/OU:ITs/CN:bee-box.bwapp.locals/O:MMEs/OU:IT
ae5fb7be864a78e168318fc1c96a4bd242c4e6c3
```

The remote host is running Linux Kernel 2.6.24-16-generic (i386)

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/0

```
Nessus SNMP scanner was able to retrieve the open port list  
with the community name: p*****  
It found 19 open TCP ports and 7 open UDP ports.
```


Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

n/a

Risk Factor

None

Plugin Information:

Published: 2005/05/15, Modified: 2017/03/13

Plugin Output

tcp/0

```
The Linux distribution detected was :  
- Ubuntu 8.04 (gutsy)
```

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:

Published: 2005/08/26, Modified: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :  
  
Nessus version : 7.1.1  
Plugin feed version : 201806151820  
Scanner edition used : Nessus  
Scan type : Normal  
Scan policy used : Basic Network Scan  
Scanner IP : 192.168.1.235  
Port scanner(s) : snmp_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 : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2018/6/19 10:51 CEST
Scan duration : 631 sec
```

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information:

Published: 2005/10/27, Modified: 2015/10/16

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```

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:

Published: 2007/05/16, Modified: 2011/03/20

Plugin Output

tcp/0

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:

Published: 2009/02/19, Modified: 2017/11/17

Plugin Output

tcp/0

```
The following card manufacturers were identified :
```

```
00:50:56:b5:1a:ad : VMware, Inc.
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was 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/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/04/21, Modified: 2017/06/06

Plugin Output

tcp/0

The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel:2.6.24.16

Following application CPE's matched on the remote system :

cpe:/a:openssl:openssl:0.9.8g -> OpenSSL Project OpenSSL 0.9.8g

cpe:/a:openbsd:openssh:4.7 -> OpenBSD OpenSSH 4.7

cpe:/a:modssl:mod_ssl:2.2.8

cpe:/a:samba:samba:3.0.28 -> Samba 3.0.28

cpe:/a:apache:http_server:2.2.8 -> Apache Software Foundation Apache HTTP Server 2.2.8

cpe:/a:php:php:5.2.4 -> PHP 5.2.4

cpe:/a:igor_sysoev:nginx:1.4.0

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:

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 98
```


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:

Published: 2013/07/08, Modified: 2018/06/12

Plugin Output

tcp/0

```
. You need to take the following 3 actions :
```

```
[ Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS (71783) ]
```

```
+ Action to take : If using NTP from the Network Time Protocol Project, upgrade to NTP version 4.2.7-p26 or later. Alternatively, add 'disable monitor' to the ntp.conf configuration file and restart the service. Otherwise, limit access to the affected service to trusted hosts, or contact the vendor for a fix.
```

```
[ OpenSSL 'ChangeCipherSpec' MiTM Vulnerability (77200) ]
```

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

```
+Impact : Taking this action will resolve 8 different vulnerabilities (CVEs).
```

```
[ Samba Badlock Vulnerability (90509) ]
```

```
+ Action to take : Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.
```

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/11/27, Modified: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.235 to 192.168.17.53 :
192.168.1.235
192.168.7.252
192.168.17.53

Hop Count: 2
```

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:

Published: 1999/10/12, Modified: 2018/02/12

Plugin Output

tcp/21

```
The remote FTP banner is :  
  
220 ProFTPD 1.3.1 Server (bee-box) [192.168.17.53]
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/21

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

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/21

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

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

<https://tools.ietf.org/html/rfc4253#section-6.3>

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

tcp/22

```
The following weak server-to-client encryption algorithms are supported :
```

```
arcfour
arcfour128
arcfour256
```

```
The following weak client-to-server encryption algorithms are supported :
```

```
arcfour
arcfour128
arcfour256
```

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

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

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.6 (CVSS2#E:ND/RL:ND/RC:ND)

References

BID	32319
CVE	CVE-2008-5161
XREF	OSVDB:50035
XREF	OSVDB:50036
XREF	CERT:958563
XREF	CWE:200

Plugin Information:

Published: 2013/10/28, Modified: 2016/05/12

Plugin Output

tcp/22

The following client-to-server Cipher Block Chaining (CBC) algorithms are supported :

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

The following server-to-client Cipher Block Chaining (CBC) algorithms are supported :

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```


71049 - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

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

Risk Factor

Low

CVSS Base Score

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

Plugin Information:

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :
```

```
  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

```
The following server-to-client Message Authentication Code (MAC) algorithms
are supported :
```

```
  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/10/12, Modified: 2017/12/19

Plugin Output

tcp/22

```
SSH version : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1  
SSH supported authentication : publickey,password
```

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/03/06, Modified: 2017/05/30

Plugin Output

tcp/22

```
The remote SSH daemon supports the following versions of the  
SSH protocol :
```

- 1.99
- 2.0

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/22

```
Port 22/tcp was found to be open
```

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/22

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

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22

```
Give Nessus credentials to perform local checks.
```

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22

```
Nessus negotiated the following encryption algorithm with the server :
```

```
The server supports the following options for kex_algorithms :
```

```
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
```

```
The server supports the following options for server_host_key_algorithms :
```

```
ssh-dss
ssh-rsa
```

```
The server supports the following options for encryption_algorithms_client_to_server :
```

```
3des-cbc
aes128-cbc
aes128-ctr
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

The server supports the following options for encryption_algorithms_server_to_client :

```
3des-cbc
aes128-cbc
aes128-ctr
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

The server supports the following options for mac_algorithms_client_to_server :

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
umac-64@openssh.com
```

The server supports the following options for mac_algorithms_server_to_client :

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
umac-64@openssh.com
```

The server supports the following options for compression_algorithms_client_to_server :

```
none
zlib@openssh.com
```

The server supports the following options for compression_algorithms_server_to_client :

```
none
zlib@openssh.com
```


15901 - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

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

Solution

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

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2004/12/03, Modified: 2016/01/08

Plugin Output

tcp/25

The SSL certificate has already expired :

```
Subject      : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office
for Complication of Otherwise Simple Affairs, CN=ubuntu, emailAddress=root@ubuntu
Issuer       : C=XX, ST=There is no such thing outside US, L=Everywhere, O=OCOSA, OU=Office
for Complication of Otherwise Simple Affairs, CN=ubuntu, emailAddress=root@ubuntu
Not valid before : Mar 28 19:14:17 2013 GMT
Not valid after  : Apr 27 19:14:17 2013 GMT
```

Synopsis

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

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>

<http://www.nessus.org/u?0bb7b67d>

<http://www.nessus.org/u?247c4540>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<http://www.nessus.org/u?5d15ba70>

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://tools.ietf.org/html/rfc7507>

<https://tools.ietf.org/html/rfc7568>

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.1 (with approved cipher suites) or higher instead.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2005/10/12, Modified: 2017/07/11

Plugin Output

tcp/25

```
- SSLv3 is enabled and the server supports at least one cipher.
```

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

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

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

See Also

<http://www.nessus.org/u?6527892d>

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

References

XREF	CWE:326
XREF	CWE:327
XREF	CWE:720
XREF	CWE:753
XREF	CWE:803
XREF	CWE:928
XREF	CWE:934

Plugin Information:

Published: 2007/10/08, Modified: 2018/05/16

Plugin Output

192.168.17.53

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

Low Strength Ciphers (<= 64-bit key)

EXP-EDH-RSA-DES-CBC-SHA	Kx=DH(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export				
EDH-RSA-DES-CBC-SHA	Kx=DH	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1
EXP-ADH-DES-CBC-SHA	Kx=DH(512)	Au=None	Enc=DES-CBC(40)	Mac=SHA1
export				
EXP-ADH-RC4-MD5	Kx=DH(512)	Au=None	Enc=RC4(40)	Mac=MD5
export				
ADH-DES-CBC-SHA	Kx=DH	Au=None	Enc=DES-CBC(56)	Mac=SHA1
EXP-DES-CBC-SHA	Kx=RSA(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export				
EXP-RC2-CBC-MD5	Kx=RSA(512)	Au=RSA	Enc=RC2-CBC(40)	Mac=MD5
export				
EXP-RC4-MD5	Kx=RSA(512)	Au=RSA	Enc=RC4(40)	Mac=MD5
export				
DES-CBC-SHA	Kx=RSA	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1

The fields above are :

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

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. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

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

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

tcp/25

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

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

EDH-RSA-DES-CBC3-SHA	Kx=DH	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
ADH-DES-CBC3-SHA	Kx=DH	Au=None	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) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/25

```
The identities known by Nessus are :
```

```
192.168.17.53
192.168.17.53
```

```
The Common Name in the certificate is :
```

```
ubuntu
```


Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that 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.

See Also

<http://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/25

The following certificate was part of the certificate chain sent by the remote host, but it has expired :

```
| -Subject    : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for  
Complication of Otherwise Simple Affairs/CN=ubuntu/E=root@ubuntu  
| -Not After  : Apr 27 19:14:17 2013 GMT
```

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

```
| -Subject : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for  
Complication of Otherwise Simple Affairs/CN=ubuntu/E=root@ubuntu  
| -Issuer  : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for  
Complication of Otherwise Simple Affairs/CN=ubuntu/E=root@ubuntu
```

Synopsis

The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.

Description

The remote SMTP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase.

Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials.

See Also

<https://tools.ietf.org/html/rfc2487>

<http://www.securityfocus.com/archive/1/516901/30/0/threaded>

Solution

Contact the vendor to see if an update is available.

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	46767
CVE	CVE-2011-0411
CVE	CVE-2011-1430
CVE	CVE-2011-1431
CVE	CVE-2011-1432
CVE	CVE-2011-1506
CVE	CVE-2011-2165
XREF	OSVDB:71020
XREF	OSVDB:71021

XREF	OSVDB:71854
XREF	OSVDB:71946
XREF	OSVDB:73251
XREF	OSVDB:75014
XREF	OSVDB:75256
XREF	CERT:555316

Plugin Information:

Published: 2011/03/10, Modified: 2017/06/12

Plugin Output

tcp/25

```
Nessus sent the following two commands in a single packet :
```

```
STARTTLS\r\nRESET\r\n
```

```
And the server sent the following two responses :
```

```
220 2.0.0 Ready to start TLS
250 2.0.0 Ok
```

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:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/25

```
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 : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
Complication of Otherwise Simple Affairs/CN=ubuntu/E=root@ubuntu
```

Synopsis

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

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

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

See Also

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00>

Solution

Disable SSLv3.

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

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	70574
CVE	CVE-2014-3566
XREF	OSVDB:113251
XREF	CERT:577193

Plugin Information:

Published: 2014/10/15, Modified: 2016/11/30

Plugin Output

tcp/25

Nessus determined that the remote server supports SSLv3 with at least one CBC cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the Fallback SCSV mechanism is not supported, allowing connections to be "rolled back" to SSLv3.

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.

See Also

<https://www.smacktls.com/#freak>

<https://www.openssl.org/news/secadv/20150108.txt>

<http://www.nessus.org/u?b78da2c4>

Solution

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	71936
CVE	CVE-2015-0204
XREF	OSVDB:116794
XREF	CERT:243585

Plugin Information:

Published: 2015/03/04, Modified: 2018/05/21

Plugin Output

tcp/25

```
EXPORT_RSA cipher suites supported by the remote server :

  Low Strength Ciphers (<= 64-bit key)

      EXP-DES-CBC-SHA           Kx=RSA(512)   Au=RSA       Enc=DES-CBC(40)   Mac=SHA1
export
      EXP-RC2-CBC-MD5          Kx=RSA(512)   Au=RSA       Enc=RC2-CBC(40)   Mac=MD5
export
      EXP-RC4-MD5              Kx=RSA(512)   Au=RSA       Enc=RC4(40)       Mac=MD5
export

The fields above are :

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

31705 - SSL Anonymous Cipher Suites Supported

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

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

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

See Also

<http://www.nessus.org/u?3a040ada>

Solution

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

Risk Factor

Low

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/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

2.3 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	28482
CVE	CVE-2007-1858
XREF	OSVDB:34882

Plugin Information:

Published: 2008/03/28, Modified: 2018/01/29

Plugin Output

tcp/25

The following is a list of SSL anonymous ciphers supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

EXP-ADH-DES-CBC-SHA	Kx=DH(512)	Au=None	Enc=DES-CBC(40)	Mac=SHA1
export				
EXP-ADH-RC4-MD5	Kx=DH(512)	Au=None	Enc=RC4(40)	Mac=MD5
export				
ADH-DES-CBC-SHA	Kx=DH	Au=None	Enc=DES-CBC(56)	Mac=SHA1

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

ADH-DES-CBC3-SHA	Kx=DH	Au=None	Enc=3DES-CBC(168)	Mac=SHA1
------------------	-------	---------	-------------------	----------

High Strength Ciphers (>= 112-bit key)

ADH-AES128-SHA	Kx=DH	Au=None	Enc=AES-CBC(128)	Mac=SHA1
ADH-AES256-SHA	Kx=DH	Au=None	Enc=AES-CBC(256)	Mac=SHA1
ADH-RC4-MD5	Kx=DH	Au=None	Enc=RC4(128)	Mac=MD5

The fields above are :

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

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:

Published: 2013/04/05, Modified: 2018/05/21

Plugin Output

tcp/25

List of RC4 cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

EXP-ADH-RC4-MD5	Kx=DH(512)	Au=None	Enc=RC4(40)	Mac=MD5
export				
EXP-RC4-MD5	Kx=RSA(512)	Au=RSA	Enc=RC4(40)	Mac=MD5
export				

High Strength Ciphers (>= 112-bit key)

ADH-RC4-MD5	Kx=DH	Au=None	Enc=RC4(128)	Mac=MD5
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}

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis

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

Description

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

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

Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

See Also

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

Solution

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

Risk Factor

Low

Plugin Information:

Published: 2013/09/03, Modified: 2014/04/10

Plugin Output

tcp/25

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

```
| -Subject      : C=XX/ST=There is no such thing outside US/L=Everywhere/O=OCOSA/OU=Office for
Complication of Otherwise Simple Affairs/CN=ubuntu/E=root@ubuntu
| -RSA Key Length : 1024 bits
```

83738 - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.

See Also

<https://weakdh.org/>

Solution

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.2 (CVSS2#E:F/RL:TF/RC:ND)

References

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

Plugin Information:

Published: 2015/05/21, Modified: 2016/06/16

Plugin Output

tcp/25

EXPORT_DHE cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

EXP-EDH-RSA-DES-CBC-SHA	Kx=DH(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export				
EXP-ADH-DES-CBC-SHA	Kx=DH(512)	Au=None	Enc=DES-CBC(40)	Mac=SHA1
export				
EXP-ADH-RC4-MD5	Kx=DH(512)	Au=None	Enc=RC4(40)	Mac=MD5
export				

The fields above are :

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

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 v3.0 Base Score

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

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:

Published: 2015/05/28, Modified: 2018/05/21

Plugin Output

tcp/25

Vulnerable connection combinations :

SSL/TLS version : TLSv1.0
Cipher suite : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Diffie-Hellman MODP size (bits) : 512
Logjam attack difficulty : Easy (could be carried out by individuals)

SSL/TLS version : SSLv3
Cipher suite : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Diffie-Hellman MODP size (bits) : 512
Logjam attack difficulty : Easy (could be carried out by individuals)

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:

Published: 1999/10/12, Modified: 2011/03/11

Plugin Output

tcp/25

```
Remote SMTP server banner :  
220 bee-box ESMTP Postfix (Ubuntu)
```

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:

Published: 2008/05/19, Modified: 2015/12/30

Plugin Output

tcp/25

```
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu
Email Address: root@ubuntu

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu
Email Address: root@ubuntu

Serial Number: 00 EC 96 38 9A F7 BD 0C D3

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 28 19:14:17 2013 GMT
Not Valid After: Apr 27 19:14:17 2013 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 1024 bits
Public Key: 00 95 E2 2B 35 F5 A2 26 E6 D3 C0 7E A0 21 22 A7 24 F3 73 93
            B8 13 81 81 37 04 EE 18 6F 6E AD 01 AD EE A3 9C D5 40 7E 92
            D5 A8 01 6C C3 1F C7 68 9E 43 5D B8 19 A3 EC 6E 04 97 0D 89
            C2 67 F2 E6 90 8A 44 86 78 90 5E DA 03 B7 18 3B 95 C5 BD 1A
            36 FC EC 41 C6 E3 67 27 A6 9A 5C 41 D5 E3 BE 8A 86 59 26 55
            36 B6 F5 77 DC C0 B2 BE 7A 47 BC 0D AE FD 2C 9E 14 AA 5A 1A
            68 42 F7 0E E3 6E 00 C4 17
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 2D 01 CE AF 06 50 12 04 61 C9 5D 04 CB 9A CE 71 00 C8 5A
            FF 3E 79 EE 8F D0 5E E5 E2 86 76 11 43 B3 9B C8 94 2E 8E 76
            6C 3D 56 D1 CF 2A 68 3E 3F 47 F8 BC B8 49 8D 8A 62 3F F8 14
            2B 90 96 B7 3E 8A A1 05 23 D0 DC 56 BD C7 AF 62 A1 10 96 25
            DE B0 DE 38 A9 2C 09 75 FF 56 BF 45 9F 31 83 1E 5E 44 D5 7B
            FA 0E 4B FC 6E 5B 02 83 3C 30 E0 DB 89 B3 E1 06 68 92 23 E9
            E7 D3 A4 F7 C3 98 E4 97 E2

Fingerprints :

SHA-256 Fingerprint: DE 61 1F 5C 49 B1 40 0E 6B 06 FF CA 0F 44 DE DD 1E A1 B4 FD
                    27 51 51 52 12 10 C6 99 CB 86 B7 B6
SHA-1 Fingerprint: D6 41 5C 57 80 28 41 45 5B 2F 5B BA 38 52 8B E4 A1 1C 2C 47
MD5 Fingerprint: 42 7E D0 25 C7 9D CB 42 B2 2D 38 7B F4 35 3C ED
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/25

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

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/man1.1.0/apps/ciphers.html>

<http://www.nessus.org/u?3a040ada>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/03/29

Plugin Output

tcp/25

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

SSL Version : TLSv1

Low Strength Ciphers (<= 64-bit key)

EXP-EDH-RSA-DES-CBC-SHA	Kx=DH(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export				
EDH-RSA-DES-CBC-SHA	Kx=DH	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1
EXP-ADH-DES-CBC-SHA	Kx=DH(512)	Au=None	Enc=DES-CBC(40)	Mac=SHA1
export				
EXP-ADH-RC4-MD5	Kx=DH(512)	Au=None	Enc=RC4(40)	Mac=MD5
export				
ADH-DES-CBC-SHA	Kx=DH	Au=None	Enc=DES-CBC(56)	Mac=SHA1
EXP-DES-CBC-SHA	Kx=RSA(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export				
EXP-RC2-CBC-MD5	Kx=RSA(512)	Au=RSA	Enc=RC2-CBC(40)	Mac=MD5
export				
EXP-RC4-MD5	Kx=RSA(512)	Au=RSA	Enc=RC4(40)	Mac=MD5
export				
DES-CBC-SHA	Kx=RSA	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

EDH-RSA-DES-CBC3-SHA	Kx=DH	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
ADH-DES-CBC3-SHA	Kx=DH	Au=None	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
ADH-AES128-SHA	Kx=DH	Au=None	Enc=AES-CBC(128)	Mac=SHA1
ADH-AES256-SHA	Kx=DH	Au=None	Enc=AES-CBC(256)	Mac=SHA1
ADH-RC4-MD5	Kx=DH	Au=None	Enc=RC4(128)	Mac=MD5
AES128-SHA	Kx=RSA	Au=RSA	[...]	

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/25

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

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

<https://en.wikipedia.org/wiki/STARTTLS>

<https://tools.ietf.org/html/rfc2487>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/10/09, Modified: 2017/06/15

Plugin Output

tcp/25

```
Here is the SMTP service's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :
```

```
----- snip -----
Subject Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
Common Name: ubuntu
Email Address: root@ubuntu

Issuer Name:

Country: XX
State/Province: There is no such thing outside US
Locality: Everywhere
Organization: OCOSA
Organization Unit: Office for Complication of Otherwise Simple Affairs
```

```
Common Name: ubuntu
Email Address: root@ubuntu

Serial Number: 00 EC 96 38 9A F7 BD 0C D3

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Mar 28 19:14:17 2013 GMT
Not Valid After: Apr 27 19:14:17 2013 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 95 E2 2B 35 F5 A2 26 E6 D3 C0 7E A0 21 22 A7 24 F3 73 93
            B8 13 81 81 37 04 EE 18 6F 6E AD 01 AD EE A3 9C D5 40 7E 92
            D5 A8 01 6C C3 1F C7 68 9E 43 5D B8 19 A3 EC 6E 04 97 0D 89
            C2 67 F2 E6 90 8A 44 86 78 90 5E DA 03 B7 18 3B 95 C5 BD 1A
            36 FC EC 41 C6 E3 67 27 A6 9A 5C 41 D5 E3 BE 8A 86 59 26 55
            36 B6 F5 77 DC C0 B2 BE 7A 47 BC 0D AE FD 2C 9E 14 AA 5A 1A
            68 42 F7 0E E3 6E 00 C4 17
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 2D 01 CE AF 06 50 12 04 61 C9 5D 04 CB 9A CE 71 00 C8 5A
            FF 3E 79 EE 8F D0 5E E5 E2 86 76 11 43 B3 9B C8 94 2E 8E 76
            6C 3D 56 D1 CF 2A 68 3E 3F 47 F8 BC B8 49 8D 8A 62 3F F8 14
            2B 90 96 B7 3E 8A A1 05 23 D0 DC 56 BD C7 AF 62 A1 10 96 25
            DE B0 DE 38 A9 2C 09 75 FF 56 BF 45 9F 31 83 1E 5E 44 D5 7B
            FA 0E 4B FC 6E 5B 02 83 3C 30 E0 DB 89 B3 E1 06 68 92 23 E9
            E7 D3 A4 F7 C3 98 E4 97 E2
```

----- snip -----

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

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

Risk Factor

None

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/25

```
The host name known by Nessus is :
```

```
bee-box
```

```
The Common Name in the certificate is :
```

```
ubuntu
```

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:

Published: 2010/11/30, Modified: 2013/10/18

Plugin Output

tcp/25

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:

Published: 2011/02/07, Modified: 2013/10/18

Plugin Output

tcp/25

```
This port supports resuming SSLv3 sessions.
```

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:

Published: 2011/12/01, Modified: 2018/02/15

Plugin Output

tcp/25

```
This port supports SSLv3/TLSv1.0.
```

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>

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/12/07, Modified: 2017/06/12

Plugin Output

tcp/25

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

Low Strength Ciphers (<= 64-bit key)

EXP-EDH-RSA-DES-CBC-SHA	Kx=DH(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export				
EDH-RSA-DES-CBC-SHA	Kx=DH	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

EDH-RSA-DES-CBC3-SHA	Kx=DH	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

The fields above are :

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

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

<http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml>

<https://tools.ietf.org/html/rfc3749>

<https://tools.ietf.org/html/rfc3943>

<https://tools.ietf.org/html/rfc5246>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2012/10/16, Modified: 2018/02/15

Plugin Output

tcp/25

```
Nessus was able to confirm that the following compression method is
supported by the target :
```

```
DEFLATE (0x01)
```

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:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/25

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

Low Strength Ciphers (<= 64-bit key)

export	EXP-EDH-RSA-DES-CBC-SHA	Kx=DH(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
	EDH-RSA-DES-CBC-SHA	Kx=DH	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1
export	EXP-ADH-DES-CBC-SHA	Kx=DH(512)	Au=None	Enc=DES-CBC(40)	Mac=SHA1
	ADH-DES-CBC-SHA	Kx=DH	Au=None	Enc=DES-CBC(56)	Mac=SHA1
export	EXP-DES-CBC-SHA	Kx=RSA(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export	EXP-RC2-CBC-MD5	Kx=RSA(512)	Au=RSA	Enc=RC2-CBC(40)	Mac=MD5
	DES-CBC-SHA	Kx=RSA	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

EDH-RSA-DES-CBC3-SHA	Kx=DH	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
ADH-DES-CBC3-SHA	Kx=DH	Au=None	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
ADH-AES128-SHA	Kx=DH	Au=None	Enc=AES-CBC(128)	Mac=SHA1
ADH-AES256-SHA	Kx=DH	Au=None	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}
```

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2018/04/24

Plugin Output

tcp/25

```
TLShv1 is enabled and the server supports at least one cipher.
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/68

```
Port 68/udp was found to be open
```

10677 - Apache mod_status /server-status Information Disclosure

Synopsis

The remote web server discloses process information.

Description

A remote unauthenticated attacker can 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.

See Also

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

Solution

Update Apache's configuration file(s) to either disable mod_status or restrict access to specific hosts.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

References

XREF OSVDB:561

Plugin Information:

Published: 2001/05/28, Modified: 2018/01/23

Plugin Output

tcp/80

```
Nessus was able to exploit the issue to retrieve the contents of
'server-status' using the following request :

http://192.168.17.53/server-status
```

Attached is a copy of the response

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:

Published: 2003/01/23, Modified: 2018/05/21

Plugin Output

tcp/80

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 /Nessus628688633.html HTTP/1.1
Connection: Close
Host: 192.168.17.53
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: Tue, 19 Jun 2018 08:56:49 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch
mod_ssl/2.2.8 OpenSSL/0.9.8g
Content-Type: message/http
X-Cache: MISS from localhost
X-Cache-Lookup: NONE from localhost:3128
Transfer-Encoding: chunked
Connection: keep-alive
```

```
TRACE /Nessus628688633.html HTTP/1.1
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
Host: 192.168.17.53
```

```
X-Forwarded-For: 192.168.1.235  
Cache-Control: max-age=259200  
Connection: keep-alive
```

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

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

See Also

<http://httpd.apache.org/docs/2.2/mod/core.html#FileETag>

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	6939
CVE	CVE-2003-1418
XREF	OSVDB:60395
XREF	CWE:200

Plugin Information:

Published: 2016/01/22, Modified: 2018/05/21

Plugin Output

tcp/80

Nessus was able to determine that the Apache Server listening on port 80 leaks the servers inode numbers in the ETag HTTP Header field :

Source	: ETag: "ccbl6-24c-506e4489b4a00"
Inode number	: 838422
File size	: 588 bytes
File modification time	: Nov. 2, 2014 at 18:20:24 GMT

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:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/80

```
The remote web server type is :
```

```
Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8  
OpenSSL/0.9.8g
```

Synopsis

A transparent or reverse HTTP proxy is running on this port.

Description

This web server is reachable through a reverse HTTP proxy.

Solution

n/a

Risk Factor

None

References

CVE	CVE-2004-2320
CVE	CVE-2005-3398
CVE	CVE-2005-3498
CVE	CVE-2007-3008
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:35511
XREF	OSVDB:50485
XREF	CWE:200
XREF	CWE:79

Plugin Information:

Published: 2002/07/02, Modified: 2018/05/21

Plugin Output

tcp/80

```
There might be a caching proxy on the way to this web server:
MISS from localhost
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/80

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


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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/80

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

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:

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/80

```
Response Code : HTTP/1.1 200 OK
```

```
Protocol version : HTTP/1.1
```

```
SSL : no
```

```
Keep-Alive : no
```

```
Options allowed : (Not implemented)
```

```
Headers :
```

```
    Date: Tue, 19 Jun 2018 08:56:44 GMT
```

```
    Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch  
mod_ssl/2.2.8 OpenSSL/0.9.8g
```

```
    Last-Modified: Sun, 02 Nov 2014 18:20:24 GMT
```

```
    ETag: "ccb16-24c-506e4489b4a00"
```

```
    Accept-Ranges: bytes
```

```
    Content-Length: 588
```

```
    Content-Type: text/html
```

```
    X-Cache: MISS from localhost
```

```
    X-Cache-Lookup: MISS from localhost:3128
```

```
    Connection: keep-alive
```

```
Response Body :
```

```
<!DOCTYPE html>
```

```
<html>
```

```
<body>
```

```
<h1>bWAPP, an extremely buggy web app !</h1>
```

```
<table>
```

```
<tr height="20">
```

```
<td>
```

```
<a href="bWAPP">bWAPP</a>
```

```
</td>
```

```
</tr>
```

```
<tr height="20">
```

```
<td>
```

```
<a href="drupal">Drupageddon</a>
```

```
</td>
```

```
</tr>
```

```
<tr height="20">
```

```
<td>
```

```
<a href="evil">Evil folder</a>
```

```
</td>
```

```
</tr>
```

```
<tr height="20">
```

```
<td>
```

```
<a href="phpmyadmin">phpMyAdmin</a>
```

```
</td>
```

```
</tr>
```

```
<tr height="20">
```

```
<td>
```

```
<a href="sqlite">SQLiteManager</a>
```

```
</td>
```

```
</tr>
```

```
<tr height="200">
```

```
<td>
```

```

```

```
</td>
```

```
</tr>
```

```
</table>
```

```
</body>
```

```
</html>
```

32318 - Web Site Cross-Domain Policy File Detection

Synopsis

The remote web server contains a 'crossdomain.xml' file.

Description

The remote web server contains a cross-domain policy file. This is a simple XML file used by Adobe's Flash Player to allow access to data that resides outside the exact web domain from which a Flash movie file originated.

See Also

<http://www.nessus.org/u?577e066f>

http://kb2.adobe.com/cps/142/tn_14213.html

<http://www.nessus.org/u?74a6a9a5>

<http://www.nessus.org/u?50ee6db2>

Solution

Review the contents of the policy file carefully. Improper policies, especially an unrestricted one with just '*', could allow for cross- site request forgery and cross-site scripting attacks against the web server.

Risk Factor

None

Plugin Information:

Published: 2008/05/15, Modified: 2017/05/16

Plugin Output

tcp/80

```
Nessus was able to obtain a cross-domain policy file from the remote
host using the following URL :
```

```
http://192.168.17.53/crossdomain.xml
```

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/80

```
Give Nessus credentials to perform local checks.
```

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:

Published: 2009/12/10, Modified: 2018/06/11

Plugin Output

tcp/80

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

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

```
/
```

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/80

```
URL      : http://192.168.17.53/
Version  : 2.2.99
backported : 1
modules  : DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8
OpenSSL/0.9.8g
os       : ConvertedUbuntu
```

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/08/04, Modified: 2017/07/07

Plugin Output

tcp/80

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

```
Version : 5.2.4-2ubuntu5  
Source  : Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-  
Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
```


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:

Published: 2011/12/16, Modified: 2016/11/18

Plugin Output

tcp/80

```
Source          : Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with
Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
Reported version : 0.9.8g
Backported version : 0.9.8g
```

84574 - Backported Security Patch Detection (PHP)

Synopsis

Security patches have been backported.

Description

Security patches may have been 'backported' to the remote PHP install without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2015/07/07, Modified: 2015/07/07

Plugin Output

tcp/80

```
Give Nessus credentials to perform local checks.
```

Synopsis

The remote NTP server is affected by a denial of service vulnerability.

Description

The version of ntpd running on the remote host has the 'monlist'

command enabled. This command returns a list of recent hosts that have connected to the service. However, it is affected by a denial of service vulnerability in ntp_request.c that allows an unauthenticated, remote attacker to saturate network traffic to a specific IP address by using forged REQ_MON_GETLIST or REQ_MON_GETLIST_1 requests.

Furthermore, an attacker can exploit this issue to conduct reconnaissance or distributed denial of service (DDoS) attacks.

See Also

<https://isc.sans.edu/diary/NTP+reflection+attack/17300>

http://bugs.ntp.org/show_bug.cgi?id=1532

<https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10613>

Solution

If using NTP from the Network Time Protocol Project, upgrade to NTP version 4.2.7-p26 or later. Alternatively, add 'disable monitor'

to the ntp.conf configuration file and restart the service. Otherwise, limit access to the affected service to trusted hosts, or contact the vendor for a fix.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.9 (CVSS:3.0/E:F/RL:O/RC:X)

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	64692
CVE	CVE-2013-5211
XREF	OSVDB:101576
XREF	CERT:348126
XREF	EDB-ID:33073
XREF	ICSA:14-051-04

Plugin Information:

Published: 2014/01/02, Modified: 2017/06/12

Plugin Output

udp/123

```
Nessus was able to retrieve the following list of recent hosts to  
connect to this NTP server :
```

```
192.168.1.235
```

Synopsis

The remote NTP server responds to mode 6 queries.

Description

The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.

See Also

<https://ntpscan.shadowserver.org>

Solution

Restrict NTP mode 6 queries.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2017/03/21, Modified: 2018/05/07

Plugin Output

udp/123

```
Nessus elicited the following response from the remote
host by sending an NTP mode 6 query :
```

```
'version="ntpd 4.2.4p4@1.1520-o Fri Mar  7 20:24:07 UTC 2008 (1)",
processor="i686", system="Linux/2.6.24-16-generic", leap=3, stratum=16,
precision=-20, rootdelay=0.000, rootdispersion=6269.775, peer=0,
refid=INIT, reftime=0x00000000.00000000, poll=6,
clock=0xded34319.753df983, state=1, offset=0.000, frequency=0.000,
jitter=0.001, noise=0.001, stability=0.000, tai=0'
```

Synopsis

An NTP server is listening on the remote host.

Description

An NTP server is listening on port 123. If not securely configured, it may provide information about its version, current date, current time, and possibly system information.

See Also

<http://www.ntp.org>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2015/03/20, Modified: 2018/05/07

Plugin Output

udp/123

```
An NTP service has been discovered, listening on port 123.
```

```
Version : 4.2.4p4
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/123

```
Port 123/udp was found to be open
```

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:

Published: 1999/10/12, Modified: 2018/06/06

Plugin Output

udp/137

The following 7 NetBIOS names have been gathered :

BEE-BOX	= Computer name
BEE-BOX	= Messenger Service
BEE-BOX	= File Server Service
__MSBROWSE__	= Master Browser
ITSECGAMES	= Master Browser
ITSECGAMES	= Browser Service Elections
ITSECGAMES	= Workgroup / Domain name

This SMB server seems to be a Samba server - its MAC address is NULL.

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/137

```
Port 137/udp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/138

```
Port 138/udp was found to be open
```

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:

Published: 2002/06/05, Modified: 2015/06/02

Plugin Output

tcp/139

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

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/139

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

41028 - SNMP Agent Default Community Name (public)

Synopsis

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

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

Disable the SNMP service on the remote host if you do not use it.

Either filter incoming UDP packets going to this port, or change the default community string.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	2112
CVE	CVE-1999-0517
XREF	OSVDB:209

Plugin Information:

Published: 2002/11/25, Modified: 2016/12/14

Plugin Output

udp/161

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

public
```


Synopsis

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

Description

The remote SNMP daemon is responding with a large amount of data to a 'GETBULK' request with a larger than normal value for 'max-repetitions'. A remote attacker can use this SNMP server to conduct a reflected distributed denial of service attack on an arbitrary remote host.

See Also

<http://www.nessus.org/u?8b551b5c>

<http://www.nessus.org/u?bdb53cfc>

Solution

Disable the SNMP service on the remote host if you do not use it.

Otherwise, restrict and monitor access to this service, and consider changing the default 'public' community string.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

4.8 (CVSS2#E:F/RL:U/RC:ND)

References

XREF OSVDB:125796

Plugin Information:

Published: 2014/07/11, Modified: 2015/09/24

Plugin Output

udp/161

Nessus was able to determine the SNMP service can be abused in an SNMP
Reflection DDoS attack :

Request size (bytes) : 42
Response size (bytes) : 2269

Synopsis

The list of processes running on the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of running processes on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.25.4.2.1.2

An attacker may use this information to gain more knowledge about the target host.

Solution

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

Risk Factor

None

Plugin Information:

Published: 2000/11/13, Modified: 2011/05/24

Plugin Output

udp/161

PID	CPU	MEM	COMMAND	ARGS
1	1	1688	init	
2	0	0	kthreadd	
3	0	0	migration/0	
4	0	0	ksoftirqd/0	
5	0	0	watchdog/0	
6	0	0	migration/1	
7	0	0	ksoftirqd/1	
8	0	0	watchdog/1	
9	0	0	migration/2	
10	0	0	ksoftirqd/2	
11	0	0	watchdog/2	
12	0	0	migration/3	
13	0	0	ksoftirqd/3	
14	0	0	watchdog/3	
15	1	0	events/0	
16	4	0	events/1	
17	1	0	events/2	
18	0	0	events/3	
19	0	0	khelper	
57	0	0	kblockd/0	
58	0	0	kblockd/1	
59	0	0	kblockd/2	
60	0	0	kblockd/3	
63	0	0	kacpid	
64	0	0	kacpi_notify	

201	0	0	kseriod
255	0	0	pdflush
256	1	0	pdflush
257	0	0	kswapd0
298	0	0	aio/0
299	0	0	aio/1
300	0	0	aio/2
301	0	0	aio/3
1713	0	0	ata/0
1714	0	0	ata/1
1719	0	0	ata/2
1720	0	0	ata/3
1724	0	0	ata_aux
1739	0	0	ksuspend_usbd
1744	0	0	khubd
2589	0	0	scsi_eh_0
2598	0	0	scsi_eh_1
2599	0	0	scsi_eh_2
2766	1	0	kjournald
2861	2	0	scsi_eh_3
2862	0	0	scsi_eh_4
2863	0	0	scsi_eh_5
2864	0	0	scsi_eh_6
2865	0	0	scsi_eh_7
2866	0	0	scsi_eh_8
2867	0	0	scsi_eh_9
2868	0	0	scsi_eh_10
2869	0	0	scsi_eh_11
2870	0	0	scsi_eh_12
2871	0	0	scsi_eh_13
2872	0	0	scsi_eh_14
2873	0	0	scsi_eh_15
2874	0		[...]

Synopsis

The list of network interfaces cards of the remote host can be obtained via SNMP.

Description

It is possible to obtain the list of the network interfaces installed on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.2.1.0

An attacker may use this information to gain more knowledge about the target host.

Solution

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

Risk Factor

None

Plugin Information:

Published: 2000/11/13, Modified: 2011/05/24

Plugin Output

udp/161

```
Interface 1 information :
ifIndex      : 1
ifDescr     : lo
ifPhysAddress :

Interface 2 information :
ifIndex      : 2
ifDescr     : eth0
ifPhysAddress : 005056b51aad
```

Synopsis

The System Information of the remote host can be obtained via SNMP.

Description

It is possible to obtain the system information about the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.1.1.

An attacker may use this information to gain more knowledge about the target host.

Solution

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

Risk Factor

None

Plugin Information:

Published: 2001/11/06, Modified: 2011/05/24

Plugin Output

udp/161

```
System information :
sysDescr      : Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i686
sysObjectID   : 1.3.6.1.4.1.8072.3.2.10
sysUptime     : 0d 11h 36m 54s
sysContact    : Your master bee
sysName       : bee-box
sysLocation   : Every bee needs a home!
sysServices   :
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/161

```
Port 161/udp was found to be open
```

Synopsis

The list of IP routes on the remote host can be obtained via SNMP.

Description

It is possible to obtain the routing information on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.4.21

An attacker may use this information to gain more knowledge about the network topology.

Solution

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

Risk Factor

None

Plugin Information:

Published: 2008/08/21, Modified: 2011/05/24

Plugin Output

udp/161

```
169.254.0.0/255.255.0.0
192.168.16.0/255.255.254.0
```

Synopsis

This plugin reports the protocol version negotiated with the remote SNMP agent.

Description

By sending an SNMP 'get-next-request', it is possible to determine the protocol version of the remote SNMP agent.

See Also

https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Solution

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

Risk Factor

None

Plugin Information:

Published: 2009/01/06, Modified: 2017/06/12

Plugin Output

udp/161

```
Nessus has negotiated SNMP communications at SNMPv2c.
```

Synopsis

This plugin reports all the protocol versions successfully negotiated with the remote SNMP agent.

Description

Extend the SNMP settings data already gathered by testing for\ SNMP versions other than the highest negotiated.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/07/31, Modified: 2013/01/19

Plugin Output

udp/161

```
This host supports SNMP version SNMPv1.  
This host supports SNMP version SNMPv2c.
```


10677 - Apache mod_status /server-status Information Disclosure

Synopsis

The remote web server discloses process information.

Description

A remote unauthenticated attacker can 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.

See Also

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

Solution

Update Apache's configuration file(s) to either disable mod_status or restrict access to specific hosts.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

References

XREF OSVDB:561

Plugin Information:

Published: 2001/05/28, Modified: 2018/01/23

Plugin Output

tcp/443

```
Nessus was able to exploit the issue to retrieve the contents of
'server-status' using the following request :
```

```
https://192.168.17.53/server-status
```

Attached is a copy of the response

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:

Published: 2003/01/23, Modified: 2018/05/21

Plugin Output

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 /Nessus645401535.html HTTP/1.1
Connection: Close
Host: 192.168.17.53
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: Tue, 19 Jun 2018 08:56:49 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch
mod_ssl/2.2.8 OpenSSL/0.9.8g
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http
```

```
TRACE /Nessus645401535.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.17.53
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 -----

Synopsis

The remote server's SSL certificate has already expired.

Description

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

Solution

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

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2004/12/03, Modified: 2016/01/08

Plugin Output

tcp/443

The SSL certificate has already expired :

```
Subject      : C=BE, ST=Flanders, L=Menen, O=MME, OU=IT, CN=bee-box.bwapp.local,
emailAddress=bwapp@itsecgames.com
Issuer       : C=BE, ST=Flanders, L=Menen, O=MME, OU=IT, CN=bee-box.bwapp.local,
emailAddress=bwapp@itsecgames.com
Not valid before : Apr 14 18:11:32 2013 GMT
Not valid after  : Apr 13 18:11:32 2018 GMT
```

Synopsis

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

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>

<http://www.nessus.org/u?0bb7b67d>

<http://www.nessus.org/u?247c4540>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<http://www.nessus.org/u?5d15ba70>

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://tools.ietf.org/html/rfc7507>

<https://tools.ietf.org/html/rfc7568>

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.1 (with approved cipher suites) or higher instead.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2005/10/12, Modified: 2017/07/11

Plugin Output

tcp/443

```
- SSLv3 is enabled and the server supports at least one cipher.
```


Synopsis

The remote service supports the use of weak SSL ciphers.

Description

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

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

See Also

<http://www.nessus.org/u?6527892d>

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

References

XREF	CWE:326
XREF	CWE:327
XREF	CWE:720
XREF	CWE:753
XREF	CWE:803
XREF	CWE:928
XREF	CWE:934

Plugin Information:

Published: 2007/10/08, Modified: 2018/05/16

Plugin Output

192.168.17.53

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

Low Strength Ciphers (<= 64-bit key)

EXP-EDH-RSA-DES-CBC-SHA	Kx=DH(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export				
EDH-RSA-DES-CBC-SHA	Kx=DH	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1
EXP-DES-CBC-SHA	Kx=RSA(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export				
EXP-RC2-CBC-MD5	Kx=RSA(512)	Au=RSA	Enc=RC2-CBC(40)	Mac=MD5
export				
EXP-RC4-MD5	Kx=RSA(512)	Au=RSA	Enc=RC4(40)	Mac=MD5
export				
DES-CBC-SHA	Kx=RSA	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1

The fields above are :

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

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

<https://tools.ietf.org/html/rfc3279>

<http://www.nessus.org/u?e120eea1>

<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

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

CVSS Temporal Score

4.3 (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:

Published: 2009/01/05, Modified: 2018/05/21

Plugin Output

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               : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/  
E=bwapp@itsecgames.com  
| -Signature Algorithm : SHA-1 With RSA Encryption  
| -Valid From           : Apr 14 18:11:32 2013 GMT  
| -Valid To             : Apr 13 18:11:32 2018 GMT
```

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. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

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

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

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, or 3DES)

EDH-RSA-DES-CBC3-SHA	Kx=DH	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) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/443

```
The identities known by Nessus are :
```

```
192.168.17.53
192.168.17.53
```

```
The Common Name in the certificate is :
```

```
bee-box.bwapp.local
```

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that 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.

See Also

<http://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/443

The following certificate was part of the certificate chain sent by the remote host, but it has expired :

```
| -Subject    : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/E=bwapp@itsecgames.com
| -Not After  : Apr 13 18:11:32 2018 GMT
```

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

```
| -Subject : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/E=bwapp@itsecgames.com
| -Issuer  : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/E=bwapp@itsecgames.com
```

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:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

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 : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/E=bwapp@itsecgames.com
```

Synopsis

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

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

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

See Also

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00>

Solution

Disable SSLv3.

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

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	70574
CVE	CVE-2014-3566
XREF	OSVDB:113251
XREF	CERT:577193

Plugin Information:

Published: 2014/10/15, Modified: 2016/11/30

Plugin Output

tcp/443

Nessus determined that the remote server supports SSLv3 with at least one CBC cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the Fallback SCSV mechanism is not supported, allowing connections to be "rolled back" to SSLv3.

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.

See Also

<https://www.smacktls.com/#freak>

<https://www.openssl.org/news/secadv/20150108.txt>

<http://www.nessus.org/u?b78da2c4>

Solution

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	71936
CVE	CVE-2015-0204
XREF	OSVDB:116794
XREF	CERT:243585

Plugin Information:

Published: 2015/03/04, Modified: 2018/05/21

Plugin Output

tcp/443

EXPORT_RSA cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

EXP-DES-CBC-SHA export	Kx=RSA(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
EXP-RC2-CBC-MD5 export	Kx=RSA(512)	Au=RSA	Enc=RC2-CBC(40)	Mac=MD5
EXP-RC4-MD5 export	Kx=RSA(512)	Au=RSA	Enc=RC4(40)	Mac=MD5

The fields above are :

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

Synopsis

The remote web server is affected by an information disclosure vulnerability.

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

See Also

<http://httpd.apache.org/docs/2.2/mod/core.html#FileETag>

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	6939
CVE	CVE-2003-1418
XREF	OSVDB:60395
XREF	CWE:200

Plugin Information:

Published: 2016/01/22, Modified: 2018/05/21

Plugin Output

tcp/443

Nessus was able to determine that the Apache Server listening on port 443 leaks the servers inode numbers in the ETag HTTP Header field :

Source	: ETag: "ccbl6-24c-506e4489b4a00"
Inode number	: 838422
File size	: 588 bytes
File modification time	: Nov. 2, 2014 at 18:20:24 GMT

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:

Published: 2013/04/05, Modified: 2018/05/21

Plugin Output

tcp/443

List of RC4 cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

EXP-RC4-MD5	Kx=RSA(512)	Au=RSA	Enc=RC4(40)	Mac=MD5
export				

High Strength Ciphers (>= 112-bit key)

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}

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis

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

Description

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

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

Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

See Also

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

Solution

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

Risk Factor

Low

Plugin Information:

Published: 2013/09/03, Modified: 2014/04/10

Plugin Output

tcp/443

The following certificates were part of the certificate chain sent by the remote host, but contain RSA keys that are considered to be weak :

```
| -Subject      : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/  
E=bwapp@itsecgames.com  
| -RSA Key Length : 1024 bits
```

83738 - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

Synopsis

The remote host supports a set of weak ciphers.

Description

The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites.

See Also

<https://weakdh.org/>

Solution

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.2 (CVSS2#E:F/RL:TF/RC:ND)

References

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

Plugin Information:

Published: 2015/05/21, Modified: 2016/06/16

Plugin Output

tcp/443

EXPORT_DHE cipher suites supported by the remote server :

Low Strength Ciphers (<= 64-bit key)

EXP-EDH-RSA-DES-CBC-SHA	Kx=DH(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export				

The fields above are :

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

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 v3.0 Base Score

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

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:

Published: 2015/05/28, Modified: 2018/05/21

Plugin Output

tcp/443

Vulnerable connection combinations :

SSL/TLS version : TLSv1.0
Cipher suite : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Diffie-Hellman MODP size (bits) : 512
Logjam attack difficulty : Easy (could be carried out by individuals)

SSL/TLS version : SSLv3
Cipher suite : TLS1_CK_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Diffie-Hellman MODP size (bits) : 512
Logjam attack difficulty : Easy (could be carried out by individuals)

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:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/443

```
The remote web server type is :
```

```
Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8  
OpenSSL/0.9.8g
```


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:

Published: 2008/05/19, Modified: 2015/12/30

Plugin Output

tcp/443

```
Subject Name:

Country: BE
State/Province: Flanders
Locality: Menen
Organization: MME
Organization Unit: IT
Common Name: bee-box.bwapp.local
Email Address: bwapp@itsecgames.com

Issuer Name:

Country: BE
State/Province: Flanders
Locality: Menen
Organization: MME
Organization Unit: IT
Common Name: bee-box.bwapp.local
Email Address: bwapp@itsecgames.com

Serial Number: 00 D8 BD 25 4A B1 5C 9F 5B

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Apr 14 18:11:32 2013 GMT
Not Valid After: Apr 13 18:11:32 2018 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 1024 bits
Public Key: 00 97 E3 6A 39 59 B2 DE 79 DB FB 42 F5 FB C1 48 60 A8 02 AC
            BF 63 E8 4D 30 AE 36 11 72 4E 6A 7C CB EA 28 F1 F6 A5 37 6A
            17 76 10 24 9C CE 28 FC 46 B3 59 83 02 7E 67 F8 67 03 7B 24
            49 50 D4 B5 E8 09 9B ED 41 F5 82 9C AA DD 54 26 4F BB 07 CA
            64 E3 AE 31 F4 DD 91 76 C7 D0 0F 77 E6 C8 C3 8F BD AB 9F 1A
            E1 2C AB 57 76 EA 44 50 77 02 57 56 B6 30 96 2F 36 4B 95 55
            E7 B6 63 91 BB 06 E6 F4 11
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 77 E0 E5 18 4A ED A2 E1 B3 D2 A0 80 8D 2B 72 BC C0 E2 DA
            2E 43 D4 B3 AE 17 31 C3 4A CB B6 B5 B9 00 2D 2C DB AE 89 76
            94 76 06 8B A8 65 CB 06 43 EB 01 70 54 EC 6C 52 08 F3 9A 55
            14 A3 00 71 98 B0 FE 09 A9 BE 0D FE 57 9B FC 8D 5A A1 EF 99
            A8 54 43 A5 52 21 26 05 A3 68 BA F5 2B AE 4E 08 61 C2 AC 10
            FE E8 8C 11 41 30 3D 73 B6 D3 03 74 74 EA B6 CF CF A7 1B BC
            43 2F 87 8C E4 05 80 6C EE

Fingerprints :

SHA-256 Fingerprint: FF 29 B3 6F CC 81 3A E5 B2 10 0D 98 5E 69 2A 61 2D E6 F1 55
                    70 37 43 20 F8 5B 43 07 6C F0 81 63
SHA-1 Fingerprint: AE 5F B7 BE 86 4A 78 E1 68 31 8F C1 C9 6A 4B D2 42 C4 E6 C3
MD5 Fingerprint:  FB EB 47 9A 22 43 50 01 3C 79 18 F7 4E C9 6F DB
```

Synopsis

The remote server is running with WebDAV enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.

It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

Solution

<http://support.microsoft.com/default.aspx?kbid=241520>

Risk Factor

None

Plugin Information:

Published: 2003/03/20, Modified: 2011/03/14

Plugin Output

tcp/443

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/443

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

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/man1.1.0/apps/ciphers.html>

<http://www.nessus.org/u?3a040ada>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/03/29

Plugin Output

tcp/443

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

SSL Version : TLSv1

Low Strength Ciphers (<= 64-bit key)

EXP-EDH-RSA-DES-CBC-SHA	Kx=DH(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export				
EDH-RSA-DES-CBC-SHA	Kx=DH	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1
EXP-DES-CBC-SHA	Kx=RSA(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export				
EXP-RC2-CBC-MD5	Kx=RSA(512)	Au=RSA	Enc=RC2-CBC(40)	Mac=MD5
export				
EXP-RC4-MD5	Kx=RSA(512)	Au=RSA	Enc=RC4(40)	Mac=MD5
export				
DES-CBC-SHA	Kx=RSA	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

EDH-RSA-DES-CBC3-SHA	Kx=DH	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
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

SSL Version : SSLv3

Low Strength Ciphers (<= 64-bit key)

EXP-EDH-RSA-DES-CBC-SHA	Kx=DH(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export				
EDH-RSA-DES-CBC-SHA	Kx=DH	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1
EXP-DES-CBC-SHA	Kx=RSA(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export	[...]			

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/443

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

tcp/443

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

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:

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/443

```
Response Code : HTTP/1.1 200 OK
```

```
Protocol version : HTTP/1.1
```

```
SSL : yes
```

```
Keep-Alive : yes
```

```
Options allowed : (Not implemented)
```

```
Headers :
```

```
    Date: Tue, 19 Jun 2018 08:56:44 GMT
```

```
    Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch  
    mod_ssl/2.2.8 OpenSSL/0.9.8g
```

```
    Last-Modified: Sun, 02 Nov 2014 18:20:24 GMT
```

```
    ETag: "ccb16-24c-506e4489b4a00"
```

```
    Accept-Ranges: bytes
```

```
    Content-Length: 588
```

```
    Keep-Alive: timeout=15, max=100
```

```
    Connection: Keep-Alive
```

```
    Content-Type: text/html
```

```
Response Body :
```

```
<!DOCTYPE html>
```

```
<html>
```

```
<body>
```

```
<h1>bwAPP, an extremely buggy web app !</h1>
```



```
<table>

  <tr height="20">
    <td>
      <a href="bWAPP">bWAPP</a>
    </td>
  </tr>

  <tr height="20">
    <td>
      <a href="drupal">Drupageddon</a>
    </td>
  </tr>

  <tr height="20">
    <td>
      <a href="evil">Evil folder</a>
    </td>
  </tr>

  <tr height="20">
    <td>
      <a href="phpmyadmin">phpMyAdmin</a>
    </td>
  </tr>

  <tr height="20">
    <td>
      <a href="sqlite">SQLiteManager</a>
    </td>
  </tr>

  <tr height="200">
    <td>
      
    </td>
  </tr>

</table>

</body>

</html>
```

32318 - Web Site Cross-Domain Policy File Detection

Synopsis

The remote web server contains a 'crossdomain.xml' file.

Description

The remote web server contains a cross-domain policy file. This is a simple XML file used by Adobe's Flash Player to allow access to data that resides outside the exact web domain from which a Flash movie file originated.

See Also

<http://www.nessus.org/u?577e066f>

http://kb2.adobe.com/cps/142/tn_14213.html

<http://www.nessus.org/u?74a6a9a5>

<http://www.nessus.org/u?50ee6db2>

Solution

Review the contents of the policy file carefully. Improper policies, especially an unrestricted one with just '*', could allow for cross- site request forgery and cross-site scripting attacks against the web server.

Risk Factor

None

Plugin Information:

Published: 2008/05/15, Modified: 2017/05/16

Plugin Output

tcp/443

```
Nessus was able to obtain a cross-domain policy file from the remote
host using the following URL :
```

```
https://192.168.17.53/crossdomain.xml
```

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/443

```
Give Nessus credentials to perform local checks.
```

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:

Published: 2009/12/10, Modified: 2018/06/11

Plugin Output

tcp/443

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

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

```
/
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

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

Risk Factor

None

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/443

```
The host name known by Nessus is :
```

```
bee-box
```

```
The Common Name in the certificate is :
```

```
bee-box.bwapp.local
```

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/07/30, Modified: 2018/01/22

Plugin Output

tcp/443

```
URL      : https://192.168.17.53/
Version  : 2.2.99
backported : 1
modules  : DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8
OpenSSL/0.9.8g
os       : ConvertedUbuntu
```

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/08/04, Modified: 2017/07/07

Plugin Output

tcp/443

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

```
Version : 5.2.4-2ubuntu5  
Source  : Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-  
Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
```

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:

Published: 2010/11/30, Modified: 2013/10/18

Plugin Output

tcp/443

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:

Published: 2011/02/07, Modified: 2013/10/18

Plugin Output

tcp/443

```
This port supports resuming SSLv3 sessions.
```

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:

Published: 2011/12/01, Modified: 2018/02/15

Plugin Output

tcp/443

```
This port supports SSLv3/TLSv1.0.
```

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>

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/12/07, Modified: 2017/06/12

Plugin Output

tcp/443

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

Low Strength Ciphers (<= 64-bit key)

EXP-EDH-RSA-DES-CBC-SHA	Kx=DH(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export				
EDH-RSA-DES-CBC-SHA	Kx=DH	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

EDH-RSA-DES-CBC3-SHA	Kx=DH	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

The fields above are :

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

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:

Published: 2011/12/16, Modified: 2016/11/18

Plugin Output

tcp/443

```
Source          : Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with  
Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g  
Reported version : 0.9.8g  
Backported version : 0.9.8g
```

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:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/443

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

Low Strength Ciphers (<= 64-bit key)

EXP-EDH-RSA-DES-CBC-SHA	Kx=DH(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export				
EDH-RSA-DES-CBC-SHA	Kx=DH	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1
EXP-DES-CBC-SHA	Kx=RSA(512)	Au=RSA	Enc=DES-CBC(40)	Mac=SHA1
export				
EXP-RC2-CBC-MD5	Kx=RSA(512)	Au=RSA	Enc=RC2-CBC(40)	Mac=MD5
export				
DES-CBC-SHA	Kx=RSA	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

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

High Strength Ciphers (\geq 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
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}

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:

Published: 2015/07/02, Modified: 2015/07/02

Plugin Output

tcp/443

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


84574 - Backported Security Patch Detection (PHP)

Synopsis

Security patches have been backported.

Description

Security patches may have been 'backported' to the remote PHP install without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2015/07/07, Modified: 2015/07/07

Plugin Output

tcp/443

```
Give Nessus credentials to perform local checks.
```

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2018/04/24

Plugin Output

tcp/443

```
TLShv1 is enabled and the server supports at least one cipher.
```

58327 - Samba 'AndX' Request Heap-Based Buffer Overflow

Synopsis

The remote Samba service is vulnerable to a heap overflow attack.

Description

The remote Samba install is prone to a heap-based buffer overflow attack.

An attacker can exploit this issue to execute arbitrary code with the privileges of the application. Failed exploit attempts will result in a denial of service condition.

See Also

<https://www.samba.org/samba/security/CVE-2012-0870.html>

<https://www.samba.org/samba/history/security.html>

Solution

Apply patches from the vendor.

Risk Factor

Critical

CVSS Base Score

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

CVSS Temporal Score

7.4 (CVSS2#E:U/RL:OF/RC:C)

References

BID	52103
CVE	CVE-2012-0870
XREF	OSVDB:79443

Plugin Information:

Published: 2012/03/13, Modified: 2018/06/06

Plugin Output

tcp/445

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 v3.0 Base Score

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

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

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:

Published: 2012/01/19, Modified: 2018/05/02

Plugin Output

tcp/445

Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability.

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists 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 who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

See Also

<http://badlock.org>

<https://www.samba.org/samba/security/CVE-2016-2118.html>

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	86002
CVE	CVE-2016-2118
XREF	OSVDB:136339
XREF	CERT:813296

Plugin Information:

Published: 2016/04/13, Modified: 2016/07/25

Plugin Output

tcp/445

Nessus detected that the Samba Badlock patch has not been applied.

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

<https://support.microsoft.com/kb/143474>

<https://support.microsoft.com/kb/246261>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/05/09, Modified: 2018/06/06

Plugin Output

tcp/445

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


Synopsis

It is possible to obtain network information.

Description

It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Solution

n/a

Risk Factor

None

References

XREF OSVDB:300

Plugin Information:

Published: 2000/05/09, Modified: 2015/01/12

Plugin Output

tcp/445

```
Here is the browse list of the remote host :  
  
BEE-BOX ( os : 0.0 )
```

Synopsis

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

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/10/17, Modified: 2017/11/30

Plugin Output

tcp/445

```
The remote Operating System is : Unix
The remote native LAN manager is : Samba 3.0.28a
The remote SMB Domain Name is : BEE-BOX
```

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:

Published: 2002/06/05, Modified: 2015/06/02

Plugin Output

tcp/445

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

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/445

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

Synopsis

An SMB server is running on the remote host.

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

See Also

<http://www.samba.org/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2007/05/16, Modified: 2013/01/07

Plugin Output

tcp/445

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

<https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>

<https://support.microsoft.com/en-us/kb/2696547>

<http://www.nessus.org/u?8dcab5e4>

<http://www.nessus.org/u?36fd3072>

<http://www.nessus.org/u?4c7e0cf3>

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF OSVDB:151058

Plugin Information:

Published: 2017/02/03, Modified: 2017/02/16

Plugin Output

tcp/445

```
The remote host supports SMBv1.
```

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2017/06/19, Modified: 2017/06/19

Plugin Output

tcp/445

```
The remote host supports the following versions of SMB :  
SMBv1
```

Synopsis

It was possible to obtain the samba version from the remote operating system.

Description

Nessus was able to obtain the samba version from the remote operating by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2017/11/30, Modified: 2017/11/30

Plugin Output

tcp/445

```
The remote Samba Version is : Samba 3.0.28a
```


Synopsis

It was possible to obtain information about the dialects of SMB2 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/02/09, Modified: 2018/02/09

Plugin Output

tcp/445

```
The remote host does NOT support the following SMB dialects :
 _version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.0         Windows 8
3.0.2       Windows 8.1
3.1         Windows 10
3.1.1       Windows 10
```

Synopsis

The rexecd service is running on the remote host.

Description

The rexecd service is running on the remote host. This service is design to allow users of a network to execute commands remotely.

However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third-party host.

Solution

Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

Risk Factor

Critical

CVSS Base Score

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

References

CVE	CVE-1999-0618
XREF	OSVDB:9721

Plugin Information:

Published: 1999/08/31, Modified: 2016/01/05

Plugin Output

tcp/512

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/512

```
Port 512/tcp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/513

```
Port 513/tcp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/514

```
Port 514/tcp was found to be open
```

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:

Published: 2002/11/18, Modified: 2016/03/24

Plugin Output

tcp/666

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      : 666
Type      : get_http
Banner    :
0x0000:  2A 2A 2A 20 62 57 41 50 50 20 4D 6F 76 69 65 20    *** bWAPP Movie
0x0010:  53 65 72 76 69 63 65 20 2A 2A 2A 0A 4D 61 74 63    Service ***,Matc
0x0020:  68 69 6E 67 20 6D 6F 76 69 65 73 3A 20 30 0A 00    hing movies: 0..
0x0030:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    .....
*
0x0400:
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/666

```
Port 666/tcp was found to be open
```

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MySQL, an open source database server.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2001/08/13, Modified: 2013/01/07

Plugin Output

tcp/3306

```
Version : 5.0.96-0ubuntu3
Protocol : 10
Server Status : SERVER_STATUS_AUTOCOMMIT
Server Capabilities :
  CLIENT_LONG_FLAG (Get all column flags)
  CLIENT_CONNECT_WITH_DB (One can specify db on connect)
  CLIENT_COMPRESS (Can use compression protocol)
  CLIENT_PROTOCOL_41 (New 4.1 protocol)
  CLIENT_TRANSACTIONS (Client knows about transactions)
  CLIENT_SECURE_CONNECTION (New 4.1 authentication)
```


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:

Published: 2002/11/18, Modified: 2017/06/08

Plugin Output

tcp/3306

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

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/3306

```
Port 3306/tcp was found to be open
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/3632

```
Port 3632/tcp was found to be open
```

12218 - mDNS Detection (Remote Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts that are not on the network segment on which Nessus resides.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2004/04/28, Modified: 2013/05/31

Plugin Output

udp/5353

Nessus was able to extract the following information :

```
- mDNS hostname      : bee-box.local.
- Advertised services :
  o Service name     : bee-box [00:50:56:b5:1a:ad]._workstation._tcp.local.
    Port number      : 9
- CPU type           : I686
- OS                  : LINUX
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/5353

```
Port 5353/udp was found to be open
```

Synopsis

The remote host is running a remote display software (VNC).

Description

The remote host is running VNC (Virtual Network Computing), which uses the RFB (Remote Framebuffer) protocol to provide remote access to graphical user interfaces and thus permits a console on the remote host to be displayed on another.

See Also

<https://en.wikipedia.org/wiki/Vnc>

Solution

Make sure use of this software is done in accordance with your organization's security policy and filter incoming traffic to this port.

Risk Factor

None

Plugin Information:

Published: 2000/03/07, Modified: 2017/06/12

Plugin Output

tcp/5901

```
The highest RFB protocol version supported by the server is :  
3.3
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/5901

```
Port 5901/tcp was found to be open
```

19288 - VNC Server Security Type Detection

Synopsis

A VNC server is running on the remote host.

Description

This script checks the remote VNC server protocol version and the available 'security types'.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2005/07/22, Modified: 2014/03/12

Plugin Output

tcp/5901

```
The remote VNC server supports the following security type :  
  2 (VNC authentication)
```


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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/5901

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

Synopsis

A VNC server with one or more unencrypted 'security-types' is running on the remote host.

Description

This script checks the remote VNC server protocol version and the available 'security types' to determine if any unencrypted 'security-types' are in use or available.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/04/03, Modified: 2014/03/12

Plugin Output

tcp/5901

```
The remote VNC server supports the following security type
which does not perform full data communication encryption :
```

```
  2 (VNC authentication)
```

10407 - X Server Detection

Synopsis

An X11 server is listening on the remote host

Description

The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client.

Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

Solution

Restrict access to this port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-nolisten tcp).

Risk Factor

Low

CVSS Base Score

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

Plugin Information:

Published: 2000/05/12, Modified: 2013/01/25

Plugin Output

tcp/6001

```
X11 Version : 11.0
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/6001

```
Port 6001/tcp was found to be open
```

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:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/8080

```
The remote web server type is :  
nginx/1.4.0
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/8080

```
Port 8080/tcp was found to be open
```

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/8080

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

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:

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/8080

```
Response Code : HTTP/1.1 200 OK

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

    Server: nginx/1.4.0
    Date: Tue, 19 Jun 2018 08:56:44 GMT
    Content-Type: text/html
    Content-Length: 588
    Last-Modified: Sun, 02 Nov 2014 18:20:24 GMT
    Connection: keep-alive
    ETag: "545675e8-24c"
    Accept-Ranges: bytes

Response Body :

<!DOCTYPE html>
<html>

<body>

<h1>bwAPP, an extremely buggy web app !</h1>

<table>
```



```
<tr height="20">
<td>
<a href="bWAPP">bWAPP</a>
</td>
</tr>

<tr height="20">
<td>
<a href="drupal">Drupageddon</a>
</td>
</tr>

<tr height="20">
<td>
<a href="evil">Evil folder</a>
</td>
</tr>

<tr height="20">
<td>
<a href="phpmyadmin">phpMyAdmin</a>
</td>
</tr>

<tr height="20">
<td>
<a href="sqlite">SQLiteManager</a>
</td>
</tr>

<tr height="200">
<td>

</td>
</tr>

</table>

</body>

</html>
```

32318 - Web Site Cross-Domain Policy File Detection

Synopsis

The remote web server contains a 'crossdomain.xml' file.

Description

The remote web server contains a cross-domain policy file. This is a simple XML file used by Adobe's Flash Player to allow access to data that resides outside the exact web domain from which a Flash movie file originated.

See Also

<http://www.nessus.org/u?577e066f>

http://kb2.adobe.com/cps/142/tn_14213.html

<http://www.nessus.org/u?74a6a9a5>

<http://www.nessus.org/u?50ee6db2>

Solution

Review the contents of the policy file carefully. Improper policies, especially an unrestricted one with just '*', could allow for cross- site request forgery and cross-site scripting attacks against the web server.

Risk Factor

None

Plugin Information:

Published: 2008/05/15, Modified: 2017/05/16

Plugin Output

tcp/8080

```
Nessus was able to obtain a cross-domain policy file from the remote
host using the following URL :
```

```
http://192.168.17.53:8080/crossdomain.xml
```

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

<https://nginx.org/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/01/26, Modified: 2018/01/26

Plugin Output

tcp/8080

```
URL      : http://192.168.17.53:8080/  
Version  : 1.4.0  
source   : Server: nginx/1.4.0
```

15901 - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

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

Solution

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

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2004/12/03, Modified: 2016/01/08

Plugin Output

tcp/8443

The SSL certificate has already expired :

```
Subject      : C=BE, ST=Flanders, L=Menen, O=MME, OU=IT, CN=bee-box.bwapp.local,
emailAddress=bwapp@itsecgames.com
Issuer       : C=BE, ST=Flanders, L=Menen, O=MME, OU=IT, CN=bee-box.bwapp.local,
emailAddress=bwapp@itsecgames.com
Not valid before : Apr 14 18:11:32 2013 GMT
Not valid after  : Apr 13 18:11:32 2018 GMT
```

Synopsis

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

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>

<http://www.nessus.org/u?0bb7b67d>

<http://www.nessus.org/u?247c4540>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<http://www.nessus.org/u?5d15ba70>

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://tools.ietf.org/html/rfc7507>

<https://tools.ietf.org/html/rfc7568>

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.1 (with approved cipher suites) or higher instead.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2005/10/12, Modified: 2017/07/11

Plugin Output

tcp/8443

```
- SSLv3 is enabled and the server supports at least one cipher.
```

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

<https://tools.ietf.org/html/rfc3279>

<http://www.nessus.org/u?e120eea1>

<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

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

CVSS Temporal Score

4.3 (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:

Published: 2009/01/05, Modified: 2018/05/21

Plugin Output

tcp/8443

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

```
| -Subject               : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/  
E=bwapp@itsecgames.com  
| -Signature Algorithm : SHA-1 With RSA Encryption  
| -Valid From           : Apr 14 18:11:32 2013 GMT  
| -Valid To             : Apr 13 18:11:32 2018 GMT
```


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. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

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

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

tcp/8443

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

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

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) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/8443

```
The identities known by Nessus are :
```

```
192.168.17.53
192.168.17.53
```

```
The Common Name in the certificate is :
```

```
bee-box.bwapp.local
```

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that 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.

See Also

<http://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/8443

The following certificate was part of the certificate chain sent by the remote host, but it has expired :

```
| -Subject    : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/E=bwapp@itsecgames.com
| -Not After  : Apr 13 18:11:32 2018 GMT
```

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

```
| -Subject : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/E=bwapp@itsecgames.com
| -Issuer  : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/E=bwapp@itsecgames.com
```

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:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/8443

```
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 : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/E=bwapp@itsecgames.com
```

Synopsis

The remote service is affected by an information disclosure vulnerability.

Description

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

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

See Also

<http://heartbleed.com/>

<http://eprint.iacr.org/2014/140>

<http://www.openssl.org/news/vulnerabilities.html#2014-0160>

<https://www.openssl.org/news/secadv/20140407.txt>

Solution

Upgrade to OpenSSL 1.0.1g or later.

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

Risk Factor

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:ND/RL:OF/RC:C)

References

BID	66690
CVE	CVE-2014-0160
XREF	OSVDB:105465
XREF	CERT:720951
XREF	EDB-ID:32745

XREF EDB-ID:32764
XREF EDB-ID:32791
XREF EDB-ID:32998

Exploitable With

Core Impact (true) Metasploit (true)

Plugin Information:

Published: 2014/04/08, Modified: 2018/05/21

Plugin Output

tcp/8443

Nessus was able to read the following memory from the remote service:

```
0x0000: 6C 54 33 00 02 3E 00 1D 00 1C FE FF FF E0 FE FE 1T3..>.....
0x0010: FF E1 00 A2 00 A3 C0 80 C0 81 C0 A6 00 AA C0 A7 .....
0x0020: 00 AB C0 96 C0 90 C0 97 C0 91 CC AD C0 9E C0 A2 .....
0x0030: 00 9E C0 9F C0 A3 00 9F C0 7C C0 7D CC AA 00 A4 .....|.}....
0x0040: 00 A5 C0 82 C0 83 00 A0 00 A1 C0 7E C0 7F 00 A6 .....~....
0x0050: 00 A7 C0 84 C0 85 C0 AC C0 AE C0 2B C0 AD C0 AF .....+....
0x0060: C0 2C C0 72 C0 86 C0 73 C0 87 CC A9 C0 9A C0 9B ..,r...s.....
0x0070: CC AC C0 2F C0 30 C0 76 C0 8A C0 77 C0 8B CC A8 .../.0.v...w...
0x0080: C0 2D C0 2E C0 74 C0 88 C0 75 C0 89 C0 31 C0 32 .-...t...u...1.2
0x0090: C0 78 C0 8C C0 79 C0 8D C0 AA C0 AB C0 A4 C0 A8 .x...y.....
0x00A0: 00 A8 C0 A5 C0 A9 00 A9 C0 94 C0 8E C0 95 C0 8F .....
0x00B0: CC AB 00 AC 00 AD C0 98 C0 92 C0 99 C0 93 CC AE .....
0x00C0: C0 9C C0 A0 00 9C C0 9D C0 A1 00 9D C0 7A C0 7B .....z.{
0x00D0: 00 63 00 65 00 11 00 13 00 32 00 38 00 44 00 87 .c.e.....2.8.D..
0x00E0: 00 12 00 66 00 99 00 8F 00 90 00 91 00 8E 00 14 ...f.....
0x00F0: 00 16 00 33 00 39 00 45 00 88 00 15 00 9A 00 0B ...3.9.E.....
0x0100: 00 0D 00 30 00 36 00 42 00 85 00 0C 00 97 00 0E ...0.6.B.....
0x0110: 00 10 00 31 00 37 00 43 00 86 00 0F 00 98 00 19 ...1.7.C.....
0x0120: 00 17 00 1B 00 34 00 3A 00 46 00 89 00 1A 00 18 ....4.:.F.....
0x0130: 00 9B C0 08 C0 09 C0 0A C0 06 C0 07 C0 12 C0 13 .....
0x0140: C0 14 C0 10 C0 11 C0 03 C0 04 C0 05 C0 01 C0 02 .....
0x0150: C0 0D C0 0E C0 0F C0 0B C0 0C C0 15 C0 17 C0 18 .....
0x0160: C0 19 C0 16 00 29 00 26 00 2A 00 27 00 2B 00 28 .....).&.*.'.+.(
0x0170: 00 23 00 1F 00 22 00 1E 00 25 00 21 00 24 00 20 .#..."...%!.$.
0x0180: 00 00 00 8B 00 8C 00 8D 00 8A 00 62 00 61 00 60 .....b.a.`
0x0190: 00 64 00 08 00 06 00 03 00 93 00 94 00 95 00 [...]

```


Synopsis

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

Description

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

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

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

- An error exists in the 'ssl3_read_bytes' function that permits data to be injected into other sessions or allows denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2010-5298)
- An error exists related to the implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) that allows nonce disclosure via the 'FLUSH+RELOAD' cache side-channel attack. (CVE-2014-0076)
- A buffer overflow error exists related to invalid DTLS fragment handling that permits the execution of arbitrary code or allows denial of service attacks.

Note that this issue only affects OpenSSL when used as a DTLS client or server. (CVE-2014-0195)

- An error exists in the 'do_ssl3_write' function that permits a NULL pointer to be dereferenced, which could allow denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2014-0198)
- An error exists related to DTLS handshake handling that could allow denial of service attacks. Note that this issue only affects OpenSSL when used as a DTLS client. (CVE-2014-0221)

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

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

See Also

<http://www.nessus.org/u?d5709faa>

<https://www.imperialviolet.org/2014/06/05/earlyccs.html>

<https://www.openssl.org/news/secadv/20140605.txt>

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

CVSS Temporal Score

5.9 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	66363
BID	66801
BID	67193
BID	67898
BID	67899
BID	67900
BID	67901
CVE	CVE-2010-5298
CVE	CVE-2014-0076
CVE	CVE-2014-0195
CVE	CVE-2014-0198
CVE	CVE-2014-0221
CVE	CVE-2014-0224
CVE	CVE-2014-3470
XREF	OSVDB:104810
XREF	OSVDB:105763
XREF	OSVDB:106531
XREF	OSVDB:107729
XREF	OSVDB:107730
XREF	OSVDB:107731
XREF	OSVDB:107732
XREF	CERT:978508

Exploitable With

Core Impact (true)

Plugin Information:

Published: 2014/08/14, Modified: 2018/06/03

Plugin Output

tcp/8443

The remote service on port 8443 accepted an early ChangeCipherSpec message, which caused the MAC and encryption keys to be derived entirely from public information. The entire SSL handshake was completed, with the server accepting and producing messages encrypted and authenticated using these weak keys.

Synopsis

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

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

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

See Also

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00>

Solution

Disable SSLv3.

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

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	70574
CVE	CVE-2014-3566
XREF	OSVDB:113251
XREF	CERT:577193

Plugin Information:

Published: 2014/10/15, Modified: 2016/11/30

Plugin Output

tcp/8443

Nessus determined that the remote server supports SSLv3 with at least one CBC cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the fallback SCSV mechanism is not supported, allowing connections to be "rolled back" to SSLv3.

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis

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

Description

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

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

Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

See Also

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

Solution

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

Risk Factor

Low

Plugin Information:

Published: 2013/09/03, Modified: 2014/04/10

Plugin Output

tcp/8443

The following certificates were part of the certificate chain sent by the remote host, but contain RSA keys that are considered to be weak :

```
| -Subject      : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/  
E=bwapp@itsecgames.com  
| -RSA Key Length : 1024 bits
```

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:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/8443

```
The remote web server type is :  
nginx/1.4.0
```

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:

Published: 2008/05/19, Modified: 2015/12/30

Plugin Output

tcp/8443

```
Subject Name:

Country: BE
State/Province: Flanders
Locality: Menen
Organization: MME
Organization Unit: IT
Common Name: bee-box.bwapp.local
Email Address: bwapp@itsecgames.com

Issuer Name:

Country: BE
State/Province: Flanders
Locality: Menen
Organization: MME
Organization Unit: IT
Common Name: bee-box.bwapp.local
Email Address: bwapp@itsecgames.com

Serial Number: 00 D8 BD 25 4A B1 5C 9F 5B

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Apr 14 18:11:32 2013 GMT
Not Valid After: Apr 13 18:11:32 2018 GMT

Public Key Info:

Algorithm: RSA Encryption
```



```
Key Length: 1024 bits
Public Key: 00 97 E3 6A 39 59 B2 DE 79 DB FB 42 F5 FB C1 48 60 A8 02 AC
            BF 63 E8 4D 30 AE 36 11 72 4E 6A 7C CB EA 28 F1 F6 A5 37 6A
            17 76 10 24 9C CE 28 FC 46 B3 59 83 02 7E 67 F8 67 03 7B 24
            49 50 D4 B5 E8 09 9B ED 41 F5 82 9C AA DD 54 26 4F BB 07 CA
            64 E3 AE 31 F4 DD 91 76 C7 D0 0F 77 E6 C8 C3 8F BD AB 9F 1A
            E1 2C AB 57 76 EA 44 50 77 02 57 56 B6 30 96 2F 36 4B 95 55
            E7 B6 63 91 BB 06 E6 F4 11
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 77 E0 E5 18 4A ED A2 E1 B3 D2 A0 80 8D 2B 72 BC C0 E2 DA
            2E 43 D4 B3 AE 17 31 C3 4A CB B6 B5 B9 00 2D 2C DB AE 89 76
            94 76 06 8B A8 65 CB 06 43 EB 01 70 54 EC 6C 52 08 F3 9A 55
            14 A3 00 71 98 B0 FE 09 A9 BE 0D FE 57 9B FC 8D 5A A1 EF 99
            A8 54 43 A5 52 21 26 05 A3 68 BA F5 2B AE 4E 08 61 C2 AC 10
            FE E8 8C 11 41 30 3D 73 B6 D3 03 74 74 EA B6 CF CF A7 1B BC
            43 2F 87 8C E4 05 80 6C EE

Fingerprints :

SHA-256 Fingerprint: FF 29 B3 6F CC 81 3A E5 B2 10 0D 98 5E 69 2A 61 2D E6 F1 55
                    70 37 43 20 F8 5B 43 07 6C F0 81 63
SHA-1 Fingerprint: AE 5F B7 BE 86 4A 78 E1 68 31 8F C1 C9 6A 4B D2 42 C4 E6 C3
MD5 Fingerprint:  FB EB 47 9A 22 43 50 01 3C 79 18 F7 4E C9 6F DB
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/8443

```
Port 8443/tcp was found to be open
```

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/man1.1.0/apps/ciphers.html>

<http://www.nessus.org/u?3a040ada>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/03/29

Plugin Output

tcp/8443

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, or 3DES)

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-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=ECDH	Au=RSA	Enc=AES-GCM(128)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-GCM(256)	Mac=SHA384
RSA-AES128-SHA256	Kx=RSA	Au=RSA	Enc=AES-GCM(128)	Mac=SHA256
RSA-AES256-SHA384	Kx=RSA	Au=RSA	Enc=AES-GCM(256)	Mac=SHA384
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
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	E [...]	

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/8443

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

tcp/8443

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

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:

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/8443

```
Response Code : HTTP/1.1 200 OK

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

    Server: nginx/1.4.0
    Date: Tue, 19 Jun 2018 08:56:44 GMT
    Content-Type: text/html
    Content-Length: 588
    Last-Modified: Sun, 02 Nov 2014 18:20:24 GMT
    Connection: keep-alive
    ETag: "545675e8-24c"
    Accept-Ranges: bytes

Response Body :

<!DOCTYPE html>
<html>

<body>

<h1>bwAPP, an extremely buggy web app !</h1>

<table>
```

```
<tr height="20">
<td>
<a href="bWAPP">bWAPP</a>
</td>
</tr>

<tr height="20">
<td>
<a href="drupal">Drupageddon</a>
</td>
</tr>

<tr height="20">
<td>
<a href="evil">Evil folder</a>
</td>
</tr>

<tr height="20">
<td>
<a href="phpmyadmin">phpMyAdmin</a>
</td>
</tr>

<tr height="20">
<td>
<a href="sqlite">SQLiteManager</a>
</td>
</tr>

<tr height="200">
<td>

</td>
</tr>

</table>

</body>

</html>
```

32318 - Web Site Cross-Domain Policy File Detection

Synopsis

The remote web server contains a 'crossdomain.xml' file.

Description

The remote web server contains a cross-domain policy file. This is a simple XML file used by Adobe's Flash Player to allow access to data that resides outside the exact web domain from which a Flash movie file originated.

See Also

<http://www.nessus.org/u?577e066f>

http://kb2.adobe.com/cps/142/tn_14213.html

<http://www.nessus.org/u?74a6a9a5>

<http://www.nessus.org/u?50ee6db2>

Solution

Review the contents of the policy file carefully. Improper policies, especially an unrestricted one with just '*', could allow for cross- site request forgery and cross-site scripting attacks against the web server.

Risk Factor

None

Plugin Information:

Published: 2008/05/15, Modified: 2017/05/16

Plugin Output

tcp/8443

```
Nessus was able to obtain a cross-domain policy file from the remote
host using the following URL :
```

```
https://192.168.17.53:8443/crossdomain.xml
```


45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

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

Risk Factor

None

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/8443

```
The host name known by Nessus is :
```

```
bee-box
```

```
The Common Name in the certificate is :
```

```
bee-box.bwapp.local
```

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:

Published: 2010/11/30, Modified: 2013/10/18

Plugin Output

tcp/8443

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:

Published: 2011/12/01, Modified: 2018/02/15

Plugin Output

tcp/8443

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

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>

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/12/07, Modified: 2017/06/12

Plugin Output

tcp/8443

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

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

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)

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=ECDH	Au=RSA	Enc=AES-GCM(128)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-GCM(256)	Mac=SHA384
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

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=ECDH	Au=RSA	Enc=AES-CBC(128)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA384

The fields above are :

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

Synopsis

The remote service advertises one or more protocols as being supported over TLS.

Description

This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections.

Note that Nessus did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and / or failing to advertise other supported protocols.

See Also

<https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04>

<https://technotes.googlecode.com/git/nextprotoneg.html>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2012/10/16, Modified: 2018/02/15

Plugin Output

tcp/8443

```
The target advertises that the following protocols are
supported over SSL / TLS :
```

```
http/1.1
```

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:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/8443

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

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

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
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
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=ECDH	Au=RSA	Enc=AES-CBC(128)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA384
RSA-AES128-SHA256	Kx=RSA	Au=RSA	Enc=AES-CBC(128)	Mac=SHA256
RSA-AES256-SHA256	Kx=RSA	Au=RSA	Enc=AES-CBC(256)	Mac=SHA256

The fields above are [...]

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:

Published: 2015/07/02, Modified: 2015/07/02

Plugin Output

tcp/8443

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

Synopsis

The remote host supports the TLS NPN extension.

Description

The remote host supports the TLS NPN (Transport Layer Security Next Protocol Negotiation) extension. This plugin enumerates the protocols the extension supports.

See Also

<https://tools.ietf.org/id/draft-agl-tls-nextprotoneg-03.html>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2015/12/08, Modified: 2015/12/08

Plugin Output

tcp/8443

```
NPN Supported Protocols:
```

```
  http/1.1
```

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2018/04/24

Plugin Output

tcp/8443

```
TLSv1 is enabled and the server supports at least one cipher.
```

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

<https://nginx.org/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/01/26, Modified: 2018/01/26

Plugin Output

tcp/8443

```
URL      : https://192.168.17.53:8443/  
Version  : 1.4.0  
source   : Server: nginx/1.4.0
```

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:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/9080

```
The remote web server type is :  
lighttpd/1.4.19
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/9080

```
Port 9080/tcp was found to be open
```

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/9080

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

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:

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/9080

```
Response Code : HTTP/1.1 200 OK

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

    Connection: close
    Vary: Accept-Encoding
    Content-Type: text/html
    Accept-Ranges: bytes
    ETag: "1762355249"
    Last-Modified: Sun, 02 Nov 2014 18:20:24 GMT
    Content-Length: 588
    Date: Tue, 19 Jun 2018 08:56:44 GMT
    Server: lighttpd/1.4.19

Response Body :

<!DOCTYPE html>
<html>

<body>

<h1>bWAPP, an extremely buggy web app !</h1>
```



```
<table>

  <tr height="20">
    <td>
      <a href="bWAPP">bWAPP</a>
    </td>
  </tr>

  <tr height="20">
    <td>
      <a href="drupal">Drupageddon</a>
    </td>
  </tr>

  <tr height="20">
    <td>
      <a href="evil">Evil folder</a>
    </td>
  </tr>

  <tr height="20">
    <td>
      <a href="phpmyadmin">phpMyAdmin</a>
    </td>
  </tr>

  <tr height="20">
    <td>
      <a href="sqlite">SQLiteManager</a>
    </td>
  </tr>

  <tr height="200">
    <td>
      
    </td>
  </tr>

</table>

</body>

</html>
```

32318 - Web Site Cross-Domain Policy File Detection

Synopsis

The remote web server contains a 'crossdomain.xml' file.

Description

The remote web server contains a cross-domain policy file. This is a simple XML file used by Adobe's Flash Player to allow access to data that resides outside the exact web domain from which a Flash movie file originated.

See Also

<http://www.nessus.org/u?577e066f>

http://kb2.adobe.com/cps/142/tn_14213.html

<http://www.nessus.org/u?74a6a9a5>

<http://www.nessus.org/u?50ee6db2>

Solution

Review the contents of the policy file carefully. Improper policies, especially an unrestricted one with just '*', could allow for cross- site request forgery and cross-site scripting attacks against the web server.

Risk Factor

None

Plugin Information:

Published: 2008/05/15, Modified: 2017/05/16

Plugin Output

tcp/9080

```
Nessus was able to obtain a cross-domain policy file from the remote
host using the following URL :
```

```
http://192.168.17.53:9080/crossdomain.xml
```

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:

Published: 2009/12/10, Modified: 2018/06/11

Plugin Output

tcp/9080

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

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

```
/
```

106628 - lighttpd HTTP Server Detection

Synopsis

The lighttpd HTTP server was detected on the remote host.

Description

Nessus was able to detect the lighttpd HTTP server by looking at the HTTP banner on the remote host.

See Also

<https://www.lighttpd.net/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/02/06, Modified: 2018/02/06

Plugin Output

tcp/9080

```
URL      : http://192.168.17.53:9080/  
Version  : 1.4.19  
source   : Server: lighttpd/1.4.19
```

Synopsis

The remote server's SSL certificate has already expired.

Description

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

Solution

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

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2004/12/03, Modified: 2016/01/08

Plugin Output

tcp/9443

The SSL certificate has already expired :

```
Subject      : C=BE, ST=Flanders, L=Menen, O=MME, OU=IT, CN=bee-box.bwapp.local,
emailAddress=bwapp@itsecgames.com
Issuer       : C=BE, ST=Flanders, L=Menen, O=MME, OU=IT, CN=bee-box.bwapp.local,
emailAddress=bwapp@itsecgames.com
Not valid before : Apr 14 18:11:32 2013 GMT
Not valid after  : Apr 13 18:11:32 2018 GMT
```

Synopsis

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

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>

<http://www.nessus.org/u?0bb7b67d>

<http://www.nessus.org/u?247c4540>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<http://www.nessus.org/u?5d15ba70>

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://tools.ietf.org/html/rfc7507>

<https://tools.ietf.org/html/rfc7568>

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.1 (with approved cipher suites) or higher instead.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2005/10/12, Modified: 2017/07/11

Plugin Output

tcp/9443

```
- SSLv3 is enabled and the server supports at least one cipher.
```

Synopsis

The remote service supports the use of weak SSL ciphers.

Description

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

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

See Also

<http://www.nessus.org/u?6527892d>

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

References

XREF	CWE:326
XREF	CWE:327
XREF	CWE:720
XREF	CWE:753
XREF	CWE:803
XREF	CWE:928
XREF	CWE:934

Plugin Information:

Published: 2007/10/08, Modified: 2018/05/16

Plugin Output

192.168.17.53

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

Low Strength Ciphers (<= 64-bit key)

DES-CBC-SHA	Kx=RSA	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1
-------------	--------	--------	-----------------	----------

The fields above are :

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

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

<https://tools.ietf.org/html/rfc3279>

<http://www.nessus.org/u?e120eea1>

<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

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

CVSS Temporal Score

4.3 (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:

Published: 2009/01/05, Modified: 2018/05/21

Plugin Output

tcp/9443

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

```
| -Subject               : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/  
E=bwapp@itsecgames.com  
| -Signature Algorithm : SHA-1 With RSA Encryption  
| -Valid From           : Apr 14 18:11:32 2013 GMT  
| -Valid To             : Apr 13 18:11:32 2018 GMT
```

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. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

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

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2009/11/23, Modified: 2017/09/01

Plugin Output

tcp/9443

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

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

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) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/9443

```
The identities known by Nessus are :
```

```
192.168.17.53
192.168.17.53
```

```
The Common Name in the certificate is :
```

```
bee-box.bwapp.local
```

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that 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.

See Also

<http://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/9443

The following certificate was part of the certificate chain sent by the remote host, but it has expired :

```
| -Subject    : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/E=bwapp@itsecgames.com
| -Not After  : Apr 13 18:11:32 2018 GMT
```

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

```
| -Subject : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/E=bwapp@itsecgames.com
| -Issuer  : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/E=bwapp@itsecgames.com
```


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:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

tcp/9443

```
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 : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/E=bwapp@itsecgames.com
```

Synopsis

The remote service has a configuration that may make it vulnerable to the CRIME attack.

Description

The remote service has one of two configurations that are known to be required for the CRIME attack :

- SSL / TLS compression is enabled.
- TLS advertises the SPDY protocol earlier than version 4.

Note that Nessus did not attempt to launch the CRIME attack against the remote service.

See Also

<http://www.iacr.org/cryptodb/data/paper.php?pubkey=3091>

<https://discussions.nessus.org/thread/5546>

<http://www.nessus.org/u?8ec18eb5>

https://issues.apache.org/bugzilla/show_bug.cgi?id=53219

Solution

Disable compression and / or the SPDY service.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	55704
BID	55707
CVE	CVE-2012-4929
CVE	CVE-2012-4930
XREF	OSVDB:85926
XREF	OSVDB:85927

Plugin Information:

Published: 2012/10/16, Modified: 2014/09/26

Plugin Output

tcp/9443

The following configuration indicates that the remote service may be vulnerable to the CRIME attack :

- SSL / TLS compression is enabled.

Synopsis

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

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

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

See Also

<https://www.imperialviolet.org/2014/10/14/poodle.html>

<https://www.openssl.org/~bodo/ssl-poodle.pdf>

<https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00>

Solution

Disable SSLv3.

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

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

3.7 (CVSS2#E:ND/RL:OF/RC:C)

References

BID	70574
CVE	CVE-2014-3566
XREF	OSVDB:113251
XREF	CERT:577193

Plugin Information:

Published: 2014/10/15, Modified: 2016/11/30

Plugin Output

tcp/9443

Nessus determined that the remote server supports SSLv3 with at least one CBC cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the Fallback SCSV mechanism is not supported, allowing connections to be "rolled back" to SSLv3.

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:

Published: 2013/04/05, Modified: 2018/05/21

Plugin Output

tcp/9443

```
List of RC4 cipher suites supported by the remote server :
```

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

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}
```

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis

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

Description

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

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

Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

See Also

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

Solution

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

Risk Factor

Low

Plugin Information:

Published: 2013/09/03, Modified: 2014/04/10

Plugin Output

tcp/9443

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

```
| -Subject      : C=BE/ST=Flanders/L=Menen/O=MME/OU=IT/CN=bee-box.bwapp.local/
E=bwapp@itsecgames.com
| -RSA Key Length : 1024 bits
```


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:

Published: 2008/05/19, Modified: 2015/12/30

Plugin Output

tcp/9443

```
Subject Name:

Country: BE
State/Province: Flanders
Locality: Menen
Organization: MME
Organization Unit: IT
Common Name: bee-box.bwapp.local
Email Address: bwapp@itsecgames.com

Issuer Name:

Country: BE
State/Province: Flanders
Locality: Menen
Organization: MME
Organization Unit: IT
Common Name: bee-box.bwapp.local
Email Address: bwapp@itsecgames.com

Serial Number: 00 D8 BD 25 4A B1 5C 9F 5B

Version: 1

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Apr 14 18:11:32 2013 GMT
Not Valid After: Apr 13 18:11:32 2018 GMT

Public Key Info:

Algorithm: RSA Encryption
```

```
Key Length: 1024 bits
Public Key: 00 97 E3 6A 39 59 B2 DE 79 DB FB 42 F5 FB C1 48 60 A8 02 AC
            BF 63 E8 4D 30 AE 36 11 72 4E 6A 7C CB EA 28 F1 F6 A5 37 6A
            17 76 10 24 9C CE 28 FC 46 B3 59 83 02 7E 67 F8 67 03 7B 24
            49 50 D4 B5 E8 09 9B ED 41 F5 82 9C AA DD 54 26 4F BB 07 CA
            64 E3 AE 31 F4 DD 91 76 C7 D0 0F 77 E6 C8 C3 8F BD AB 9F 1A
            E1 2C AB 57 76 EA 44 50 77 02 57 56 B6 30 96 2F 36 4B 95 55
            E7 B6 63 91 BB 06 E6 F4 11
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 77 E0 E5 18 4A ED A2 E1 B3 D2 A0 80 8D 2B 72 BC C0 E2 DA
            2E 43 D4 B3 AE 17 31 C3 4A CB B6 B5 B9 00 2D 2C DB AE 89 76
            94 76 06 8B A8 65 CB 06 43 EB 01 70 54 EC 6C 52 08 F3 9A 55
            14 A3 00 71 98 B0 FE 09 A9 BE 0D FE 57 9B FC 8D 5A A1 EF 99
            A8 54 43 A5 52 21 26 05 A3 68 BA F5 2B AE 4E 08 61 C2 AC 10
            FE E8 8C 11 41 30 3D 73 B6 D3 03 74 74 EA B6 CF CF A7 1B BC
            43 2F 87 8C E4 05 80 6C EE

Fingerprints :

SHA-256 Fingerprint: FF 29 B3 6F CC 81 3A E5 B2 10 0D 98 5E 69 2A 61 2D E6 F1 55
                    70 37 43 20 F8 5B 43 07 6C F0 81 63
SHA-1 Fingerprint: AE 5F B7 BE 86 4A 78 E1 68 31 8F C1 C9 6A 4B D2 42 C4 E6 C3
MD5 Fingerprint:  FB EB 47 9A 22 43 50 01 3C 79 18 F7 4E C9 6F DB
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

tcp/9443

```
Port 9443/tcp was found to be open
```

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/man1.1.0/apps/ciphers.html>

<http://www.nessus.org/u?3a040ada>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/03/29

Plugin Output

tcp/9443

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

SSL Version : TLSv1

Low Strength Ciphers (<= 64-bit key)

DES-CBC-SHA	Kx=RSA	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1
-------------	--------	--------	-----------------	----------

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

DES-CBC3-SHA	Kx=RSA	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
--------------	--------	--------	-------------------	----------

High Strength Ciphers (>= 112-bit key)

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

SSL Version : SSLv3

Low Strength Ciphers (<= 64-bit key)

DES-CBC-SHA	Kx=RSA	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)				
DES-CBC3-SHA	Kx=RSA	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
High Strength Ciphers (>= 112-bit key)				
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}
```

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/9443

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

tcp/9443

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

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

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

Risk Factor

None

Plugin Information:

Published: 2010/04/03, Modified: 2017/06/05

Plugin Output

tcp/9443

```
The host name known by Nessus is :
```

```
bee-box
```

```
The Common Name in the certificate is :
```

```
bee-box.bwapp.local
```

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:

Published: 2010/11/30, Modified: 2013/10/18

Plugin Output

tcp/9443

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:

Published: 2011/02/07, Modified: 2013/10/18

Plugin Output

tcp/9443

```
This port supports resuming SSLv3 sessions.
```

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:

Published: 2011/12/01, Modified: 2018/02/15

Plugin Output

tcp/9443

```
This port supports SSLv3/TLSv1.0.
```

Synopsis

The remote service supports one or more compression methods for SSL connections.

Description

This script detects which compression methods are supported by the remote service for SSL connections.

See Also

<http://www.iana.org/assignments/comp-meth-ids/comp-meth-ids.xml>

<https://tools.ietf.org/html/rfc3749>

<https://tools.ietf.org/html/rfc3943>

<https://tools.ietf.org/html/rfc5246>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2012/10/16, Modified: 2018/02/15

Plugin Output

tcp/9443

```
Nessus was able to confirm that the following compression method is
supported by the target :
```

```
  DEFLATE (0x01)
```

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:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/9443

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

Low Strength Ciphers (<= 64-bit key)

DES-CBC-SHA	Kx=RSA	Au=RSA	Enc=DES-CBC(56)	Mac=SHA1
-------------	--------	--------	-----------------	----------

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

DES-CBC3-SHA	Kx=RSA	Au=RSA	Enc=3DES-CBC(168)	Mac=SHA1
--------------	--------	--------	-------------------	----------

High Strength Ciphers (>= 112-bit key)

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}
```

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information:

Published: 2017/11/22, Modified: 2018/04/24

Plugin Output

tcp/9443

```
TLSv1 is enabled and the server supports at least one cipher.
```

Synopsis

SNMP information is enumerated to learn about other open ports.

Description

This plugin runs an SNMP scan against the remote machine to find open ports.

See the section 'plugins options' to configure it.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/08/15, Modified: 2018/01/29

Plugin Output

udp/36242

```
Port 36242/udp was found to be open
```


192.168.17.252

0

CRITICAL

0

HIGH

3

MEDIUM

0

LOW

47

INFO

Scan Information

Start time: Tue Jun 19 11:49:26 2018

End time: Tue Jun 19 11:58:29 2018

Host Information

IP: 192.168.17.252

OS: FreeBSD 11.1-RELEASE-p7 (amd64)

Vulnerabilities

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:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -1 seconds.
```

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:

Published: 2003/12/09, Modified: 2018/04/19

Plugin Output

tcp/0

```
Remote operating system : FreeBSD 11.1-RELEASE-p7 (amd64)
Confidence level : 98
Method : NTP
```

```
The remote host is running FreeBSD 11.1-RELEASE-p7 (amd64)
```

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:

Published: 2005/08/26, Modified: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :  
  
Nessus version : 7.1.1  
Plugin feed version : 201806151820  
Scanner edition used : Nessus  
Scan type : Normal  
Scan policy used : Basic Network Scan  
Scanner IP : 192.168.1.252  
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 : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2018/6/19 11:49 CEST
Scan duration : 520 sec
```

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:

Published: 2007/05/16, Modified: 2011/03/20

Plugin Output

tcp/0

Synopsis

It was 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/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/04/21, Modified: 2017/06/06

Plugin Output

tcp/0

The remote operating system matched the following CPE :

`cpe:/o:freebsd:freebsd:11.1`

Following application CPE matched on the remote system :

`cpe:/a:openbsd:openssh:7.2`

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:

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 98
```


Synopsis

The remote host is a firewall.

Description

The remote host is pfSense, an open source firewall based on FreeBSD.

It is possible to read the version by either using SNMP or viewing the web interface after logging in.

See Also

<https://www.pfsense.org/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/02/22, Modified: 2018/05/21

Plugin Output

tcp/0

```
Source : HTTPS
Version : unknown
```

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/11/27, Modified: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.235 to 192.168.17.252 :  
192.168.1.235  
192.168.17.252  
  
Hop Count: 1
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/10/12, Modified: 2017/12/19

Plugin Output

tcp/22

```
SSH version : SSH-2.0-OpenSSH_7.2
SSH supported authentication : publickey,password,keyboard-interactive
```

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/03/06, Modified: 2017/05/30

Plugin Output

tcp/22

```
The remote SSH daemon supports the following versions of the
SSH protocol :
```

- 1.99
- 2.0

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/22

```
Port 22/tcp was found to be open
```

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/22

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

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22

```
Give Nessus credentials to perform local checks.
```

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22

```
Nessus negotiated the following encryption algorithm with the server :
```

```
The server supports the following options for kex_algorithms :
```

```
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
```

```
The server supports the following options for server_host_key_algorithms :
```

```
rsa-sha2-256
rsa-sha2-512
ssh-ed25519
ssh-rsa
```

```
The server supports the following options for encryption_algorithms_client_to_server :
```

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

```
The server supports the following options for encryption_algorithms_server_to_client :
```

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
```



```
aes256-gcm@openssh.com  
chacha20-poly1305@openssh.com
```

The server supports the following options for mac_algorithms_client_to_server :

```
hmac-ripemd160  
hmac-ripemd160-etm@openssh.com  
hmac-sha2-256  
hmac-sha2-256-etm@openssh.com  
hmac-sha2-512  
hmac-sha2-512-etm@openssh.com  
umac-128-etm@openssh.com  
umac-128@openssh.com
```

The server supports the following options for mac_algorithms_server_to_client :

```
hmac-ripemd160  
hmac-ripemd160-etm@openssh.com  
hmac-sha2-256  
hmac-sha2-256-etm@openssh.com  
hmac-sha2-512  
hmac-sha2-512-etm@openssh.com  
umac-128-etm@openssh.com  
umac-128@openssh.com
```

The server supports the following options for compression_algorithms_client_to_server :

```
none  
zlib@openssh.com
```

The server supports the following options for compression_algorithms_server_to_client :

```
none  
zlib@openssh.com
```

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:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/80

```
The remote web server type is :  
nginx
```

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/04/28, Modified: 2015/10/13

Plugin Output

tcp/80

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 301
rather than 404. The requested URL was :
```

```
http://192.168.17.252/qoEmYlPJJeUDl.html
```

Synopsis

A transparent or reverse HTTP proxy is running on this port.

Description

This web server is reachable through a reverse HTTP proxy.

Solution

n/a

Risk Factor

None

References

CVE	CVE-2004-2320
CVE	CVE-2005-3398
CVE	CVE-2005-3498
CVE	CVE-2007-3008
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:35511
XREF	OSVDB:50485
XREF	CWE:200
XREF	CWE:79

Plugin Information:

Published: 2002/07/02, Modified: 2018/05/21

Plugin Output

tcp/80

```
There might be a caching proxy on the way to this web server:
MISS from localhost
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/80

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

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/80

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

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:

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/80

```
Response Code : HTTP/1.1 301 Moved Permanently
```

```
Protocol version : HTTP/1.1
```

```
SSL : no
```

```
Keep-Alive : no
```

```
Options allowed : (Not implemented)
```

```
Headers :
```

```
    Server: nginx
```

```
    Date: Tue, 19 Jun 2018 09:55:55 GMT
```

```
    Content-Type: text/html
```

```
    Content-Length: 178
```

```
    Location: https://192.168.17.252/
```

```
    X-Frame-Options: SAMEORIGIN
```

```
    X-Cache: MISS from localhost
```

```
    X-Cache-Lookup: MISS from localhost:3128
```

```
    Connection: keep-alive
```

```
Response Body :
```

```
<html>
```

```
<head><title>301 Moved Permanently</title></head>
```

```
<body bgcolor="white">
```

```
<center><h1>301 Moved Permanently</h1></center>
```

```
<hr><center>nginx</center>
```

```
</body>
```

```
</html>
```


Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

<https://nginx.org/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/01/26, Modified: 2018/01/26

Plugin Output

tcp/80

```
URL      : http://192.168.17.252/  
Version  : unknown  
source   : Server: nginx
```

Synopsis

The remote NTP server responds to mode 6 queries.

Description

The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.

See Also

<https://ntpscan.shadowserver.org>

Solution

Restrict NTP mode 6 queries.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2017/03/21, Modified: 2018/05/07

Plugin Output

udp/123

```
Nessus elicited the following response from the remote
host by sending an NTP mode 6 query :
```

```
'version="ntpd 4.2.8p11@1.3728-o Fri Mar 16 18:58:06 UTC 2018 (1)",
processor="amd64", system="FreeBSD/11.1-RELEASE-p7", leap=0, stratum=3,
precision=-21, rootdelay=18.756, rootdisp=32.088, refid=5.196.160.139,
reftime=0xded34bad.46c586df, clock=0xded350ca.f8f5331f, peer=10688,
tc=9, mintc=3, offset=-0.061290, frequency=-20.739, sys_jitter=0.214190,
clk_jitter=0.145, clk_wander=0.007'
```

Synopsis

An NTP server is listening on the remote host.

Description

An NTP server is listening on port 123. If not securely configured, it may provide information about its version, current date, current time, and possibly system information.

See Also

<http://www.ntp.org>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2015/03/20, Modified: 2018/05/07

Plugin Output

udp/123

```
An NTP service has been discovered, listening on port 123.  
Version : 4.2.8p11
```

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that 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.

See Also

<http://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/443

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

```
| -Subject : C=LU/ST=Luxembourg/L=Esch_sur_alzette/O=Sags/E=sags@telindus.lu/CN=CA_LAB  
| -Issuer  : C=LU/ST=Luxembourg/L=Esch_sur_alzette/O=Sags/E=sags@telindus.lu/CN=CA_LAB
```

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:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

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 : C=LU/ST=Luxembourg/L=Esch_sur_alzette/O=Sags/E=sags@telindus.lu/CN=CA_LAB
```

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:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/443

```
The remote web server type is :  
nginx
```

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:

Published: 2008/05/19, Modified: 2015/12/30

Plugin Output

tcp/443

```
Subject Name:

Country: LU
State/Province: Luxembourg
Locality: Esch_sur_alzette
Organization: Sags
Email Address: sags@telindus.lu
Common Name: Piffil.sags.lu

Issuer Name:

Country: LU
State/Province: Luxembourg
Locality: Esch_sur_alzette
Organization: Sags
Email Address: sags@telindus.lu
Common Name: iCA_WEB

Serial Number: 01

Version: 3

Signature Algorithm: SHA-512 With RSA Encryption

Not Valid Before: Jul 11 15:44:42 2017 GMT
Not Valid After: Jul 11 15:44:42 2019 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 D3 4F 06 D8 14 C6 C8 38 9E 4F 98 AA 43 2D AF FA 5E EA 9F
```



```
DE 8A 7A 7E 06 8D 4D 4C DA 76 34 51 B7 28 F6 50 24 86 D2 CD
E8 00 F7 8F 80 33 C9 12 23 89 7F 5A 3E A1 BE 66 15 21 1F 16
A4 E0 47 27 CB 2D FD E3 B7 99 D6 7A E5 F4 B0 35 29 2C 31 C2
9A F9 65 DD F9 0B 2D 42 60 37 1B 25 C6 9B 57 8E 54 F5 FA B2
4D 3D 18 6C 37 94 35 89 57 B3 6D 8C D5 65 A0 20 85 0A 88 56
28 00 F9 21 37 D0 09 2D 46 A6 96 3A 2F 4D 22 87 AE A1 D1 41
F3 69 CC 15 32 83 FD AA 4D 13 2F 53 FD AD 57 FC 83 2E 98 DD
AA 07 F6 4E F6 EB BC E2 9D 21 3C 3D 40 B0 5E 58 5C 42 4E A4
A4 DF 70 DC 04 4B 25 B5 E7 63 6C C5 4C F5 CF F0 4F CB 57 EA
3E 72 63 81 78 6E CF 8C 65 5B 4F 4D AF 0E 82 68 7D 49 39 3F
86 7C 4A 0F 43 F6 FB E4 37 5C 25 83 F6 7E 62 89 B7 A6 2B FE
A4 BC C8 B9 D0 A7 CE F3 30 FB A7 D0 ED 07 8F 25 F6 28 48 41
59 0F A4 6E FB 99 97 60 EB 0D 32 D2 A2 74 10 05 68 85 35 11
3E 74 03 60 65 2E CA 1C 2C 1E 0B DE 0C E8 4E 1F 6F 80 CF 6C
4F F0 98 B0 37 7E A7 01 A9 5F D5 06 AB 30 F9 3A 7B 0E 52 F4
34 41 88 37 95 9B 66 E2 B5 CF 6B 04 D8 CA 1F 73 B6 36 B8 F1
E4 35 64 8F 9A CC 71 E0 6C 1A 8B 1B 25 CB D3 22 BD 53 FC 78
88 93 46 C6 8F 89 A2 3B 57 07 79 E3 E8 4F EE F5 32 E5 F3 AA
99 2E AE 30 6F 10 9B FA 36 96 70 FB 85 F1 7C 2E FC 3D D4 BA
A5 96 D9 BC 30 EB AA E0 DD [...]
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/443

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

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/man1.1.0/apps/ciphers.html>

<http://www.nessus.org/u?3a040ada>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/03/29

Plugin Output

tcp/443

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

SSL Version : TLSv12

High Strength Ciphers (>= 112-bit key)

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=ECDH	Au=RSA	Enc=AES-GCM(128)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-GCM(256)	Mac=SHA384
DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
ECDHE-RSA-AES256-SHA	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
DHE-RSA-AES256-SHA256	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA384

SSL Version : TLSv11

High Strength Ciphers (>= 112-bit key)

DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	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}
```

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/443

```
A TLSv1.1 server answered on this port.
```

tcp/443

```
A web server is running on this port through TLSv1.1.
```

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:

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/443

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1

SSL : yes

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Server: nginx

Date: Tue, 19 Jun 2018 09:55:56 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

X-Frame-Options: SAMEORIGIN

Last-Modified: Tue, 19 Jun 2018 09:55:56 GMT

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Strict-Transport-Security: max-age=31536000

X-Content-Type-Options: nosniff

Response Body :

<!DOCTYPE html>

<html lang="en">

<head>

<meta name="viewport" content="width=device-width, initial-scale=1">

```

    <link rel="stylesheet" href="/vendor/bootstrap/css/bootstrap.min.css" type="text/css">
    <link rel="stylesheet" href="/css/login.css?v=1521486180" type="text/css">
<title>Login</title>
<script type="text/javascript">
  //

```

42822 - Strict Transport Security (STS) Detection

Synopsis

The remote web server implements Strict Transport Security.

Description

The remote web server implements Strict Transport Security (STS).

The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.

All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

See Also

<http://www.nessus.org/u?2fb3aca6>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/11/16, Modified: 2013/11/19

Plugin Output

tcp/443

```
The STS header line is :  
Strict-Transport-Security: max-age=31536000
```


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:

Published: 2011/12/01, Modified: 2018/02/15

Plugin Output

tcp/443

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

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>

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/12/07, Modified: 2017/06/12

Plugin Output

tcp/443

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

High Strength Ciphers (>= 112-bit key)

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=ECDH	Au=RSA	Enc=AES-GCM(128)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-GCM(256)	Mac=SHA384
DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
ECDHE-RSA-AES256-SHA	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
DHE-RSA-AES256-SHA256	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA384

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}

```
Au={authentication}  
Enc={symmetric encryption method}  
Mac={message authentication code}  
{export flag}
```

Synopsis

The remote service advertises one or more protocols as being supported over TLS.

Description

This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections.

Note that Nessus did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and / or failing to advertise other supported protocols.

See Also

<https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04>

<https://technotes.googlecode.com/git/nextprotoneg.html>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2012/10/16, Modified: 2018/02/15

Plugin Output

tcp/443

```
The target advertises that the following protocols are
supported over SSL / TLS :
```

```
http/1.1
```

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:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/443

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

High Strength Ciphers (>= 112-bit key)

DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
ECDHE-RSA-AES256-SHA	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
DHE-RSA-AES256-SHA256	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA384

The fields above are :

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

```
{export flag}
```

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:

Published: 2015/07/17, Modified: 2016/02/15

Plugin Output

tcp/443

```
ALPN Supported Protocols:
```

```
  http/1.1
```

Synopsis

The remote host supports the TLS NPN extension.

Description

The remote host supports the TLS NPN (Transport Layer Security Next Protocol Negotiation) extension. This plugin enumerates the protocols the extension supports.

See Also

<https://tools.ietf.org/id/draft-agl-tls-nextprotoneg-03.html>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2015/12/08, Modified: 2015/12/08

Plugin Output

tcp/443

```
NPN Supported Protocols:
```

```
  http/1.1
```


Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

<https://technet.microsoft.com/en-us/library/cc778623>

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Published: 2016/11/14, Modified: 2016/11/14

Plugin Output

tcp/443

The following root Certification Authority certificate was found :

```
| -Subject          : C=LU/ST=Luxembourg/L=Esch_sur_alzette/O=Sags/E=sags@telindus.lu/CN=CA_LAB
| -Issuer           : C=LU/ST=Luxembourg/L=Esch_sur_alzette/O=Sags/E=sags@telindus.lu/CN=CA_LAB
| -Valid From       : Jun 16 07:30:18 2017 GMT
| -Valid To         : Jun 11 07:30:18 2037 GMT
| -Signature Algorithm : SHA-512 With RSA Encryption
```

Synopsis

The web interface for a firewall was detected on the remote host.

Description

The web interface for pfSense was detected on the remote host.

pfSense is an open source firewall based on FreeBSD.

See Also

<https://www.pfsense.org/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/01/19, Modified: 2018/06/15

Plugin Output

tcp/443

```
URL      : https://192.168.17.252/
Version  : unknown
Note     : Please specify HTTP username and password to retrieve version information.
```

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

<https://nginx.org/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/01/26, Modified: 2018/01/26

Plugin Output

tcp/443

```
URL      : https://192.168.17.252/  
Version  : unknown  
source   : Server: nginx
```

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

<https://jquery.com/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/02/07, Modified: 2018/02/07

Plugin Output

tcp/443

```
URL      : https://192.168.17.252/vendor/jquery/jquery-1.12.0.min.js?v=1521486180
Version  : 1.12.0
```

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:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/3128

```
The remote web server type is :  
squid/3.5.27
```

Synopsis

An HTTP proxy running on the remote host can be used to establish interactive sessions.

Description

The proxy allows users to perform CONNECT requests such as :

CONNECT http://cvs.example.org:23

This request gives the person who made it the ability to have an interactive session with a third-party site.

This issue may allow attackers to bypass your firewall by connecting to sensitive ports such as 23 (telnet) via the proxy, or it may allow internal users to bypass the firewall rules and connect to ports or sites they should not be allowed to.

In addition, your proxy may be used to perform attacks against other networks.

Solution

Reconfigure your proxy to refuse CONNECT requests.

Risk Factor

None

Plugin Information:

Published: 1999/06/22, Modified: 2016/04/27

Plugin Output

tcp/3128

10195 - HTTP Proxy Open Relay Detection

Synopsis

The remote web proxy server accepts requests.

Description

The remote web proxy accepts unauthenticated HTTP requests from the Nessus scanner. By routing requests through the affected proxy, a user may be able to gain some degree of anonymity while browsing websites, which will see requests as originating from the remote host itself rather than the user's host.

Solution

Make sure access to the proxy is limited to valid users / hosts.

Risk Factor

None

Plugin Information:

Published: 1999/06/22, Modified: 2014/04/25

Plugin Output

tcp/3128

Synopsis

A transparent or reverse HTTP proxy is running on this port.

Description

This web server is reachable through a reverse HTTP proxy.

Solution

n/a

Risk Factor

None

References

CVE	CVE-2004-2320
CVE	CVE-2005-3398
CVE	CVE-2005-3498
CVE	CVE-2007-3008
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:35511
XREF	OSVDB:50485
XREF	CWE:200
XREF	CWE:79

Plugin Information:

Published: 2002/07/02, Modified: 2018/05/21

Plugin Output

tcp/3128

```
There might be a caching proxy on the way to this web server:
MISS from localhost
```


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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/3128

```
Port 3128/tcp was found to be open
```

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/3128

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

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:

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/3128

```
Response Code : HTTP/1.1 400 Bad Request
```

```
Protocol version : HTTP/1.1
```

```
SSL : no
```

```
Keep-Alive : no
```

```
Options allowed : (Not implemented)
```

```
Headers :
```

```
    Server: squid/3.5.27
```

```
    Mime-Version: 1.0
```

```
    Date: Tue, 19 Jun 2018 09:55:56 GMT
```

```
    Content-Type: text/html; charset=utf-8
```

```
    Content-Length: 3548
```

```
    X-Squid-Error: ERR_INVALID_URL 0
```

```
    Vary: Accept-Language
```

```
    Content-Language: fr
```

```
    X-Cache: MISS from localhost
```

```
    X-Cache-Lookup: NONE from localhost:3128
```

```
    Connection: close
```

```
Response Body :
```

```
<html><head>
```

```
<meta type="copyright" content="Copyright (C) 1996-2017 The Squid Software Foundation and  
  contributors">
```

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
```

```

<title>ERREUR : l'URL demand.e n'a pas pu ..tre charg..e</title>
<style type="text/css"><!--
/*
 * Copyright (C) 1996-2017 The Squid Software Foundation and contributors
 *
 * Squid software is distributed under GPLv2+ license and includes
 * contributions from numerous individuals and organizations.
 * Please see the COPYING and CONTRIBUTORS files for details.
 */

/*
  Stylesheet for Squid Error pages
  Adapted from design by Free CSS Templates
  http://www.freecsstemplates.org
  Released for free under a Creative Commons Attribution 2.5 License
 */

/* Page basics */
* {
  font-family: verdana, sans-serif;
}

html body {
  margin: 0;
  padding: 0;
  background: #efefef;
  font-size: 12px;
  color: #1e1e1e;
}

/* Page displayed title area */
#titles {
  margin-left: 15px;
  padding: 10px;
  padding-left: 100px;
  background: url('/squid-internal-static/icons/SN.png') no-repeat left;
}

/* initial title */
#titles h1 {
  color: #000000;
}
#titles h2 {
  color: #000000;
}

/* special event: FTP success page titles */
#titles ftpsuccess {
  background-color: #00ff00;
  width: 100%;
}

/* Page displayed body content area */
#content {
  padding: 10px;
  background: #ffffff;
}

/* General text */
p {
}

/* error brief description */
#error p {
}

/* some data which may have caused the problem */
#data {
}

```

```
/* the error message received from the system or other software */  
#sysms [...]
```

Synopsis

It was possible to obtain the version number of the remote Squid proxy server.

Description

The remote host is running the Squid proxy server, an open source proxy server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/09/28, Modified: 2015/04/02

Plugin Output

tcp/3128

```
Source  : Squid  
Version : 3.5.27
```


192.168.17.253

0

CRITICAL

0

HIGH

2

MEDIUM

0

LOW

27

INFO

Scan Information

Start time: Tue Jun 19 11:49:26 2018

End time: Tue Jun 19 12:03:49 2018

Host Information

IP: 192.168.17.253

OS: pfSense

Vulnerabilities

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:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -39 seconds.
```

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:

Published: 2003/12/09, Modified: 2018/04/19

Plugin Output

tcp/0

```
Remote operating system : pfSense
Confidence level : 70
Method : SinFP
```

```
The remote host is running pfSense
```

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:

Published: 2005/08/26, Modified: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :  
  
Nessus version : 7.1.1  
Plugin feed version : 201806151820  
Scanner edition used : Nessus  
Scan type : Normal  
Scan policy used : Basic Network Scan  
Scanner IP : 192.168.1.252  
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 : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2018/6/19 11:49 CEST
Scan duration : 839 sec
```

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:

Published: 2007/05/16, Modified: 2011/03/20

Plugin Output

tcp/0

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:

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : firewall  
Confidence level : 70
```

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/11/27, Modified: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.235 to 192.168.17.253 :  
192.168.1.235  
192.168.7.252  
192.168.17.253
```

```
Hop Count: 2
```

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/03/06, Modified: 2017/05/30

Plugin Output

tcp/22

```
The remote SSH daemon supports the following versions of the  
SSH protocol :
```

```
- 1.99
```


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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/22

```
Port 22/tcp was found to be open
```

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/22

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

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22

```
Nessus negotiated the following encryption algorithm with the server :
```

```
The server supports the following options for kex_algorithms :
```

```
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
```

```
The server supports the following options for server_host_key_algorithms :
```

```
rsa-sha2-256
rsa-sha2-512
ssh-ed25519
ssh-rsa
```

```
The server supports the following options for encryption_algorithms_client_to_server :
```

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

```
The server supports the following options for encryption_algorithms_server_to_client :
```

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
```

```
aes256-gcm@openssh.com  
chacha20-poly1305@openssh.com
```

The server supports the following options for mac_algorithms_client_to_server :

```
hmac-ripemd160  
hmac-ripemd160-etm@openssh.com  
hmac-sha2-256  
hmac-sha2-256-etm@openssh.com  
hmac-sha2-512  
hmac-sha2-512-etm@openssh.com  
umac-128-etm@openssh.com  
umac-128@openssh.com
```

The server supports the following options for mac_algorithms_server_to_client :

```
hmac-ripemd160  
hmac-ripemd160-etm@openssh.com  
hmac-sha2-256  
hmac-sha2-256-etm@openssh.com  
hmac-sha2-512  
hmac-sha2-512-etm@openssh.com  
umac-128-etm@openssh.com  
umac-128@openssh.com
```

The server supports the following options for compression_algorithms_client_to_server :

```
none  
zlib@openssh.com
```

The server supports the following options for compression_algorithms_server_to_client :

```
none  
zlib@openssh.com
```

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:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/80

```
The remote web server type is :  
nginx
```

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/04/28, Modified: 2015/10/13

Plugin Output

tcp/80

```
CGI scanning will be disabled for this host because the host responds  
to requests for non-existent URLs with HTTP code 301  
rather than 404. The requested URL was :
```

```
http://192.168.17.253/buqn5rsME3BS.html
```

Synopsis

A transparent or reverse HTTP proxy is running on this port.

Description

This web server is reachable through a reverse HTTP proxy.

Solution

n/a

Risk Factor

None

References

CVE	CVE-2004-2320
CVE	CVE-2005-3398
CVE	CVE-2005-3498
CVE	CVE-2007-3008
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:35511
XREF	OSVDB:50485
XREF	CWE:200
XREF	CWE:79

Plugin Information:

Published: 2002/07/02, Modified: 2018/05/21

Plugin Output

tcp/80

```
There might be a caching proxy on the way to this web server:
MISS from localhost
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/80

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


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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/80

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

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:

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/80

```
Response Code : HTTP/1.1 301 Moved Permanently
```

```
Protocol version : HTTP/1.1
```

```
SSL : no
```

```
Keep-Alive : no
```

```
Options allowed : (Not implemented)
```

```
Headers :
```

```
    Server: nginx
```

```
    Date: Tue, 19 Jun 2018 09:57:29 GMT
```

```
    Content-Type: text/html
```

```
    Content-Length: 178
```

```
    Location: https://192.168.17.253/
```

```
    X-Frame-Options: SAMEORIGIN
```

```
    X-Cache: MISS from localhost
```

```
    X-Cache-Lookup: MISS from localhost:3128
```

```
    Connection: keep-alive
```

```
Response Body :
```

```
<html>
```

```
<head><title>301 Moved Permanently</title></head>
```

```
<body bgcolor="white">
```

```
<center><h1>301 Moved Permanently</h1></center>
```

```
<hr><center>nginx</center>
```

```
</body>
```

</html>

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

<https://nginx.org/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/01/26, Modified: 2018/01/26

Plugin Output

tcp/80

```
URL      : http://192.168.17.253/  
Version  : unknown  
source   : Server: nginx
```

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that 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.

See Also

<http://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/443

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

```
| -Subject : C=LU/ST=Luxembourg/L=Esch_sur_alzette/O=Sags/E=sags@telindus.lu/CN=CA_LAB  
| -Issuer  : C=LU/ST=Luxembourg/L=Esch_sur_alzette/O=Sags/E=sags@telindus.lu/CN=CA_LAB
```

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:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

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 : C=LU/ST=Luxembourg/L=Esch_sur_alzette/O=Sags/E=sags@telindus.lu/CN=CA_LAB
```

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:

Published: 2008/05/19, Modified: 2015/12/30

Plugin Output

tcp/443

```
Subject Name:

Country: LU
State/Province: Luxembourg
Locality: Esch_sur_alzette
Organization: Sags
Email Address: sags@telindus.lu
Common Name: Piffi2.sags.lu

Issuer Name:

Country: LU
State/Province: Luxembourg
Locality: Esch_sur_alzette
Organization: Sags
Email Address: sags@telindus.lu
Common Name: iCA_WEB

Serial Number: 02

Version: 3

Signature Algorithm: SHA-512 With RSA Encryption

Not Valid Before: Jul 11 15:44:48 2017 GMT
Not Valid After: Aug 30 15:44:48 2019 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 DB 59 72 E5 A6 EA C5 2B F6 9D 00 4A D6 CC EF 6D 12 FB 75
```



```
3A 70 B7 E5 8D 2E A3 E1 DD 37 C0 96 AF 8D D9 E3 98 A1 7E 54
CA 2F 6C 69 24 17 56 FB D9 43 D2 FA 61 B4 6C CA 26 01 5E F2
E1 B2 3E 20 2B C0 70 6A 94 70 35 E1 31 68 BF E2 CC 9C FC 4D
92 B2 5C B5 EA 6E BD 3A ED 18 F9 09 27 D1 41 B3 7B 3D 4C 42
56 D5 43 95 B3 DB DC E8 CE 25 E7 FA FD 68 C5 E9 8F D5 D1 18
FE 99 D4 72 B2 97 D9 33 CB B6 3C 24 32 7F 63 35 FB 6D 0B 95
E9 82 9E B7 F6 C3 DB 46 94 E8 F0 4B BE 8C 84 A9 37 7C 76 B4
3C DC FF 7E DE 48 FB 1C 0F 3A 11 85 F2 EB 48 F2 A6 B3 94 6E
42 2E CD FB 31 01 A8 DB F3 C7 F1 D2 4D A1 17 E6 43 E3 10 EA
8D A1 BE D5 56 79 9F 74 D8 98 19 13 6C 8E B2 E4 3A D9 4D 67
E4 2C E0 CF 6F 3D AD C8 7B A3 0E 33 C6 95 E0 F2 20 0A 6F 87
11 76 F7 FE D3 9A D2 4F 0A 1D 64 A5 E6 EB 65 34 46 44 A3 5A
4F 2C F7 7E FC 5E 9F 04 1C D0 7B 6B 10 3A 6F 28 F9 E6 D5 73
6D 01 C6 C4 EC ED E4 DA CA 2F 2A F5 BF D0 B3 DA D1 B6 DB 4D
81 8A E8 2F 60 EE 99 EA 23 47 9A A7 0B CF 61 C4 B8 2B 42 35
7F FF 98 90 54 DF D4 7A D5 0D 83 66 1C 6A ED 6A 00 11 C2 6A
B2 A8 5B CA AD 09 03 B9 AB 5E 45 C7 C7 82 EC 28 05 04 84 C1
51 63 16 78 52 BB 04 78 65 70 CC 95 26 42 0C 78 08 8B 5E 93
24 89 E6 12 C7 37 AB B3 40 49 79 84 96 72 02 EF 31 11 43 40
B3 B1 20 6F E2 DE 47 18 23 [...]
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/443

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

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/man1.1.0/apps/ciphers.html>

<http://www.nessus.org/u?3a040ada>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/03/29

Plugin Output

tcp/443

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

SSL Version : TLSv12

High Strength Ciphers (>= 112-bit key)

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=ECDH	Au=RSA	Enc=AES-GCM(128)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-GCM(256)	Mac=SHA384
DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
DHE-RSA-AES256-SHA256	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA384

SSL Version : TLSv11

High Strength Ciphers (>= 112-bit key)

DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	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}
```

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/443

```
A TLSv1.1 server answered on this port.
```

tcp/443

```
A web server is running on this port through TLSv1.1.
```

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:

Published: 2011/12/01, Modified: 2018/02/15

Plugin Output

tcp/443

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

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>

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/12/07, Modified: 2017/06/12

Plugin Output

tcp/443

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

High Strength Ciphers (>= 112-bit key)

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=ECDH	Au=RSA	Enc=AES-GCM(128)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-GCM(256)	Mac=SHA384
DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
ECDHE-RSA-AES256-SHA	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
DHE-RSA-AES256-SHA256	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA384

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}

```
Au={authentication}  
Enc={symmetric encryption method}  
Mac={message authentication code}  
{export flag}
```


Synopsis

The remote service advertises one or more protocols as being supported over TLS.

Description

This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections.

Note that Nessus did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and / or failing to advertise other supported protocols.

See Also

<https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04>

<https://technotes.googlecode.com/git/nextprotoneg.html>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2012/10/16, Modified: 2018/02/15

Plugin Output

tcp/443

```
The target advertises that the following protocols are
supported over SSL / TLS :
```

```
http/1.1
```

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:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/443

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

High Strength Ciphers (>= 112-bit key)

DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
ECDHE-RSA-AES256-SHA	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
DHE-RSA-AES256-SHA256	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA384

The fields above are :

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

```
{export flag}
```

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:

Published: 2015/07/17, Modified: 2016/02/15

Plugin Output

tcp/443

```
ALPN Supported Protocols:
```

```
  http/1.1
```

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

<https://technet.microsoft.com/en-us/library/cc778623>

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Published: 2016/11/14, Modified: 2016/11/14

Plugin Output

tcp/443

The following root Certification Authority certificate was found :

```
| -Subject          : C=LU/ST=Luxembourg/L=Esch_sur_alzette/O=Sags/E=sags@telindus.lu/CN=CA_LAB
| -Issuer           : C=LU/ST=Luxembourg/L=Esch_sur_alzette/O=Sags/E=sags@telindus.lu/CN=CA_LAB
| -Valid From       : Jun 16 07:30:18 2017 GMT
| -Valid To         : Jun 11 07:30:18 2037 GMT
| -Signature Algorithm : SHA-512 With RSA Encryption
```


192.168.17.254

0

CRITICAL

0

HIGH

3

MEDIUM

0

LOW

39

INFO

Scan Information

Start time: Tue Jun 19 11:49:35 2018

End time: Tue Jun 19 11:58:17 2018

Host Information

IP: 192.168.17.254

OS: FreeBSD 11.1-RELEASE-p7 (amd64)

Vulnerabilities

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:

Published: 1999/08/01, Modified: 2012/06/18

Plugin Output

icmp/0

```
The remote clock is synchronized with the local clock.
```


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:

Published: 2003/12/09, Modified: 2018/04/19

Plugin Output

tcp/0

```
Remote operating system : FreeBSD 11.1-RELEASE-p7 (amd64)
Confidence level : 98
Method : NTP
```

```
The remote host is running FreeBSD 11.1-RELEASE-p7 (amd64)
```

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:

Published: 2005/08/26, Modified: 2017/10/26

Plugin Output

tcp/0

```
Information about this scan :  
  
Nessus version : 7.1.1  
Plugin feed version : 201806151820  
Scanner edition used : Nessus  
Scan type : Normal  
Scan policy used : Basic Network Scan  
Scanner IP : 192.168.1.252  
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 : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2018/6/19 11:49 CEST
Scan duration : 499 sec
```

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:

Published: 2007/05/16, Modified: 2011/03/20

Plugin Output

tcp/0

Synopsis

It was 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/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2010/04/21, Modified: 2017/06/06

Plugin Output

tcp/0

The remote operating system matched the following CPE :

`cpe:/o:freebsd:freebsd:11.1`

Following application CPE matched on the remote system :

`cpe:/a:openbsd:openssh:7.2`

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:

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 98
```

Synopsis

The remote host is a firewall.

Description

The remote host is pfSense, an open source firewall based on FreeBSD.

It is possible to read the version by either using SNMP or viewing the web interface after logging in.

See Also

<https://www.pfsense.org/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/02/22, Modified: 2018/05/21

Plugin Output

tcp/0

```
Source : HTTPS
Version : unknown
```

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/11/27, Modified: 2017/08/22

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.1.235 to 192.168.17.254 :  
192.168.1.235  
192.168.17.254  
  
Hop Count: 1
```


10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 1999/10/12, Modified: 2017/12/19

Plugin Output

tcp/22

```
SSH version : SSH-2.0-OpenSSH_7.2
SSH supported authentication : publickey,password,keyboard-interactive
```

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2002/03/06, Modified: 2017/05/30

Plugin Output

tcp/22

```
The remote SSH daemon supports the following versions of the  
SSH protocol :
```

- 1.99
- 2.0

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/22

```
Port 22/tcp was found to be open
```

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/22

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

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22

```
Give Nessus credentials to perform local checks.
```

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22

```
Nessus negotiated the following encryption algorithm with the server :
```

```
The server supports the following options for kex_algorithms :
```

```
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
```

```
The server supports the following options for server_host_key_algorithms :
```

```
rsa-sha2-256
rsa-sha2-512
ssh-ed25519
ssh-rsa
```

```
The server supports the following options for encryption_algorithms_client_to_server :
```

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

```
The server supports the following options for encryption_algorithms_server_to_client :
```

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
```

```
aes256-gcm@openssh.com  
chacha20-poly1305@openssh.com
```

The server supports the following options for mac_algorithms_client_to_server :

```
hmac-ripemd160  
hmac-ripemd160-etm@openssh.com  
hmac-sha2-256  
hmac-sha2-256-etm@openssh.com  
hmac-sha2-512  
hmac-sha2-512-etm@openssh.com  
umac-128-etm@openssh.com  
umac-128@openssh.com
```

The server supports the following options for mac_algorithms_server_to_client :

```
hmac-ripemd160  
hmac-ripemd160-etm@openssh.com  
hmac-sha2-256  
hmac-sha2-256-etm@openssh.com  
hmac-sha2-512  
hmac-sha2-512-etm@openssh.com  
umac-128-etm@openssh.com  
umac-128@openssh.com
```

The server supports the following options for compression_algorithms_client_to_server :

```
none  
zlib@openssh.com
```

The server supports the following options for compression_algorithms_server_to_client :

```
none  
zlib@openssh.com
```

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:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/80

```
The remote web server type is :  
nginx
```


Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2000/04/28, Modified: 2015/10/13

Plugin Output

tcp/80

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 301
rather than 404. The requested URL was :
```

```
http://192.168.17.254/YlZFG4alU3np.html
```

Synopsis

A transparent or reverse HTTP proxy is running on this port.

Description

This web server is reachable through a reverse HTTP proxy.

Solution

n/a

Risk Factor

None

References

CVE	CVE-2004-2320
CVE	CVE-2005-3398
CVE	CVE-2005-3498
CVE	CVE-2007-3008
XREF	OSVDB:877
XREF	OSVDB:3726
XREF	OSVDB:35511
XREF	OSVDB:50485
XREF	CWE:200
XREF	CWE:79

Plugin Information:

Published: 2002/07/02, Modified: 2018/05/21

Plugin Output

tcp/80

```
There might be a caching proxy on the way to this web server:
MISS from localhost
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/80

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

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/80

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

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:

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/80

```
Response Code : HTTP/1.1 301 Moved Permanently
```

```
Protocol version : HTTP/1.1
```

```
SSL : no
```

```
Keep-Alive : no
```

```
Options allowed : (Not implemented)
```

```
Headers :
```

```
    Server: nginx
```

```
    Date: Tue, 19 Jun 2018 09:56:02 GMT
```

```
    Content-Type: text/html
```

```
    Content-Length: 178
```

```
    Location: https://192.168.17.254/
```

```
    X-Frame-Options: SAMEORIGIN
```

```
    X-Cache: MISS from localhost
```

```
    X-Cache-Lookup: MISS from localhost:3128
```

```
    Connection: keep-alive
```

```
Response Body :
```

```
<html>
```

```
<head><title>301 Moved Permanently</title></head>
```

```
<body bgcolor="white">
```

```
<center><h1>301 Moved Permanently</h1></center>
```

```
<hr><center>nginx</center>
```

```
</body>
```

```
</html>
```

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

<https://nginx.org/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/01/26, Modified: 2018/01/26

Plugin Output

tcp/80

```
URL      : http://192.168.17.254/  
Version  : unknown  
source   : Server: nginx
```

Synopsis

The remote NTP server responds to mode 6 queries.

Description

The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.

See Also

<https://ntpscan.shadowserver.org>

Solution

Restrict NTP mode 6 queries.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2017/03/21, Modified: 2018/05/07

Plugin Output

udp/123

Nessus elicited the following response from the remote host by sending an NTP mode 6 query :

```
'version="ntpd 4.2.8p11@1.3728-o Fri Mar 16 18:58:06 UTC 2018 (1)",
processor="amd64", system="FreeBSD/11.1-RELEASE-p7", leap=0, stratum=3,
precision=-21, rootdelay=18.756, rootdisp=32.148, refid=5.196.160.139,
reftime=0xded34bad.46c586df, clock=0xded350ce.4f428e46, peer=10688,
tc=9, mintc=3, offset=-0.061290, frequency=-20.739, sys_jitter=0.214190,
clk_jitter=0.145, clk_wander=0.007'
```


Synopsis

An NTP server is listening on the remote host.

Description

An NTP server is listening on port 123. If not securely configured, it may provide information about its version, current date, current time, and possibly system information.

See Also

<http://www.ntp.org>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2015/03/20, Modified: 2018/05/07

Plugin Output

udp/123

```
An NTP service has been discovered, listening on port 123.  
Version : 4.2.8p11
```

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that 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.

See Also

<http://www.itu.int/rec/T-REC-X.509/en>

<https://en.wikipedia.org/wiki/X.509>

Solution

Purchase or generate a proper certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Published: 2010/12/15, Modified: 2017/05/18

Plugin Output

tcp/443

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

```
| -Subject : C=LU/ST=Luxembourg/L=Esch_sur_alzette/O=Sags/E=sags@telindus.lu/CN=CA_LAB  
| -Issuer  : C=LU/ST=Luxembourg/L=Esch_sur_alzette/O=Sags/E=sags@telindus.lu/CN=CA_LAB
```

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:

Published: 2012/01/17, Modified: 2016/12/14

Plugin Output

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 : C=LU/ST=Luxembourg/L=Esch_sur_alzette/O=Sags/E=sags@telindus.lu/CN=CA_LAB
```

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:

Published: 2000/01/04, Modified: 2018/05/23

Plugin Output

tcp/443

```
The remote web server type is :  
nginx
```

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:

Published: 2008/05/19, Modified: 2015/12/30

Plugin Output

tcp/443

```
Subject Name:

Country: LU
State/Province: Luxembourg
Locality: Esch_sur_alzette
Organization: Sags
Email Address: sags@telindus.lu
Common Name: Piffil.sags.lu

Issuer Name:

Country: LU
State/Province: Luxembourg
Locality: Esch_sur_alzette
Organization: Sags
Email Address: sags@telindus.lu
Common Name: iCA_WEB

Serial Number: 01

Version: 3

Signature Algorithm: SHA-512 With RSA Encryption

Not Valid Before: Jul 11 15:44:42 2017 GMT
Not Valid After: Jul 11 15:44:42 2019 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 4096 bits
Public Key: 00 D3 4F 06 D8 14 C6 C8 38 9E 4F 98 AA 43 2D AF FA 5E EA 9F
```

```
DE 8A 7A 7E 06 8D 4D 4C DA 76 34 51 B7 28 F6 50 24 86 D2 CD
E8 00 F7 8F 80 33 C9 12 23 89 7F 5A 3E A1 BE 66 15 21 1F 16
A4 E0 47 27 CB 2D FD E3 B7 99 D6 7A E5 F4 B0 35 29 2C 31 C2
9A F9 65 DD F9 0B 2D 42 60 37 1B 25 C6 9B 57 8E 54 F5 FA B2
4D 3D 18 6C 37 94 35 89 57 B3 6D 8C D5 65 A0 20 85 0A 88 56
28 00 F9 21 37 D0 09 2D 46 A6 96 3A 2F 4D 22 87 AE A1 D1 41
F3 69 CC 15 32 83 FD AA 4D 13 2F 53 FD AD 57 FC 83 2E 98 DD
AA 07 F6 4E F6 EB BC E2 9D 21 3C 3D 40 B0 5E 58 5C 42 4E A4
A4 DF 70 DC 04 4B 25 B5 E7 63 6C C5 4C F5 CF F0 4F CB 57 EA
3E 72 63 81 78 6E CF 8C 65 5B 4F 4D AF 0E 82 68 7D 49 39 3F
86 7C 4A 0F 43 F6 FB E4 37 5C 25 83 F6 7E 62 89 B7 A6 2B FE
A4 BC C8 B9 D0 A7 CE F3 30 FB A7 D0 ED 07 8F 25 F6 28 48 41
59 0F A4 6E FB 99 97 60 EB 0D 32 D2 A2 74 10 05 68 85 35 11
3E 74 03 60 65 2E CA 1C 2C 1E 0B DE 0C E8 4E 1F 6F 80 CF 6C
4F F0 98 B0 37 7E A7 01 A9 5F D5 06 AB 30 F9 3A 7B 0E 52 F4
34 41 88 37 95 9B 66 E2 B5 CF 6B 04 D8 CA 1F 73 B6 36 B8 F1
E4 35 64 8F 9A CC 71 E0 6C 1A 8B 1B 25 CB D3 22 BD 53 FC 78
88 93 46 C6 8F 89 A2 3B 57 07 79 E3 E8 4F EE F5 32 E5 F3 AA
99 2E AE 30 6F 10 9B FA 36 96 70 FB 85 F1 7C 2E FC 3D D4 BA
A5 96 D9 BC 30 EB AA E0 DD [...]
```

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:

Published: 2009/02/04, Modified: 2017/05/22

Plugin Output

tcp/443

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


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/man1.1.0/apps/ciphers.html>

<http://www.nessus.org/u?3a040ada>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2006/06/05, Modified: 2018/03/29

Plugin Output

tcp/443

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

SSL Version : TLSv12

High Strength Ciphers (>= 112-bit key)

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=ECDH	Au=RSA	Enc=AES-GCM(128)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-GCM(256)	Mac=SHA384
DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
ECDHE-RSA-AES256-SHA	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
DHE-RSA-AES256-SHA256	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA384

SSL Version : TLSv11

High Strength Ciphers (>= 112-bit key)

DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	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}
```

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:

Published: 2007/08/19, Modified: 2018/05/03

Plugin Output

tcp/443

```
A TLSv1.1 server answered on this port.
```

tcp/443

```
A web server is running on this port through TLSv1.1.
```

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:

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/443

```
Response Code : HTTP/1.1 200 OK

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

    Server: nginx
    Date: Tue, 19 Jun 2018 09:56:02 GMT
    Content-Type: text/html; charset=UTF-8
    Transfer-Encoding: chunked
    Connection: keep-alive
    X-Frame-Options: SAMEORIGIN
    Last-Modified: Tue, 19 Jun 2018 09:56:02 GMT
    Expires: Thu, 19 Nov 1981 08:52:00 GMT
    Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
    Pragma: no-cache
    Strict-Transport-Security: max-age=31536000
    X-Content-Type-Options: nosniff

Response Body :

<!DOCTYPE html>
<html lang="en">
<head>
  <meta name="viewport" content="width=device-width, initial-scale=1">
```

```

    <link rel="stylesheet" href="/vendor/bootstrap/css/bootstrap.min.css" type="text/css">
    <link rel="stylesheet" href="/css/login.css?v=1521486180" type="text/css">
<title>Login</title>
<script type="text/javascript">
  //

```

42822 - Strict Transport Security (STS) Detection

Synopsis

The remote web server implements Strict Transport Security.

Description

The remote web server implements Strict Transport Security (STS).

The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.

All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

See Also

<http://www.nessus.org/u?2fb3aca6>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/11/16, Modified: 2013/11/19

Plugin Output

tcp/443

```
The STS header line is :
```

```
Strict-Transport-Security: max-age=31536000
```

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:

Published: 2011/12/01, Modified: 2018/02/15

Plugin Output

tcp/443

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

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>

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

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

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2011/12/07, Modified: 2017/06/12

Plugin Output

tcp/443

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

High Strength Ciphers (>= 112-bit key)

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=ECDH	Au=RSA	Enc=AES-GCM(128)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-GCM(256)	Mac=SHA384
DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
ECDHE-RSA-AES256-SHA	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
DHE-RSA-AES256-SHA256	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA384

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}


```
Au={authentication}  
Enc={symmetric encryption method}  
Mac={message authentication code}  
{export flag}
```

Synopsis

The remote service advertises one or more protocols as being supported over TLS.

Description

This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections.

Note that Nessus did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and / or failing to advertise other supported protocols.

See Also

<https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04>

<https://technotes.googlecode.com/git/nextprotoneg.html>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2012/10/16, Modified: 2018/02/15

Plugin Output

tcp/443

```
The target advertises that the following protocols are
supported over SSL / TLS :
```

```
http/1.1
```

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:

Published: 2013/10/22, Modified: 2013/10/22

Plugin Output

tcp/443

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

High Strength Ciphers (>= 112-bit key)

DHE-RSA-AES256-SHA	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
ECDHE-RSA-AES256-SHA	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA1
DHE-RSA-AES256-SHA256	Kx=DH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA256
ECDHE-RSA-AES256-SHA384	Kx=ECDH	Au=RSA	Enc=AES-CBC(256)	Mac=SHA384

The fields above are :

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

```
{export flag}
```

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:

Published: 2015/07/17, Modified: 2016/02/15

Plugin Output

tcp/443

```
ALPN Supported Protocols:
```

```
  http/1.1
```

Synopsis

The remote host supports the TLS NPN extension.

Description

The remote host supports the TLS NPN (Transport Layer Security Next Protocol Negotiation) extension. This plugin enumerates the protocols the extension supports.

See Also

<https://tools.ietf.org/id/draft-agl-tls-nextprotoneg-03.html>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2015/12/08, Modified: 2015/12/08

Plugin Output

tcp/443

```
NPN Supported Protocols:
```

```
  http/1.1
```

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

<https://technet.microsoft.com/en-us/library/cc778623>

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Published: 2016/11/14, Modified: 2016/11/14

Plugin Output

tcp/443

The following root Certification Authority certificate was found :

```
| -Subject          : C=LU/ST=Luxembourg/L=Esch_sur_alzette/O=Sags/E=sags@telindus.lu/CN=CA_LAB
| -Issuer           : C=LU/ST=Luxembourg/L=Esch_sur_alzette/O=Sags/E=sags@telindus.lu/CN=CA_LAB
| -Valid From       : Jun 16 07:30:18 2017 GMT
| -Valid To         : Jun 11 07:30:18 2037 GMT
| -Signature Algorithm : SHA-512 With RSA Encryption
```

Synopsis

The web interface for a firewall was detected on the remote host.

Description

The web interface for pfSense was detected on the remote host.

pfSense is an open source firewall based on FreeBSD.

See Also

<https://www.pfsense.org/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/01/19, Modified: 2018/06/15

Plugin Output

tcp/443

```
URL      : https://192.168.17.254/
Version  : unknown
Note     : Please specify HTTP username and password to retrieve version information.
```


Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

<https://nginx.org/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/01/26, Modified: 2018/01/26

Plugin Output

tcp/443

```
URL      : https://192.168.17.254/  
Version  : unknown  
source   : Server: nginx
```

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

<https://jquery.com/>

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2018/02/07, Modified: 2018/02/07

Plugin Output

tcp/443

```
URL      : https://192.168.17.254/vendor/jquery/jquery-1.12.0.min.js?v=1521486180
Version  : 1.12.0
```

Remediations

Suggested Remediations

Taking the following actions across 2 hosts would resolve 7% of the vulnerabilities on the network.

ACTION TO TAKE	VULNS	HOSTS
OpenSSL 'ChangeCipherSpec' MiTM Vulnerability: OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za. OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m. OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h.	8	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	2	2
Apache HTTP Server httpOnly Cookie Information Disclosure: Upgrade to Apache version 2.0.65 / 2.2.22 or later.	1	1
Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS: If using NTP from the Network Time Protocol Project, upgrade to NTP version 4.2.7-p26 or later. Alternatively, add 'disable monitor' to the ntp.conf configuration file and restart the service. Otherwise, limit access to the affected service to trusted hosts, or contact the vendor for a fix.	1	1