Advanced Scan Connected Pakistan

Report generated by Tenable Nessus™ Wed, 16 Jul 2025 18:20:01 PKT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

connectedpakistan.pk

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	2	135

Scan Information

Start time: Wed Jul 16 17:32:04 2025
End time: Wed Jul 16 18:20:01 2025

Host Information

DNS Name: connectedpakistan.pk
IP: 5.9.177.100
OS: Linux Kernel 2.6

Vulnerabilities

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

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

Solution

Configure the remote web server to use HSTS.

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 v2.0 Base Score

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

Plugin Information

Published: 2020/11/17, Modified: 2024/03/22

Plugin Output

tcp/2083/www

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Wed, 16 Jul 2025 12:37:36 GMT
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
Set-Cookie: cpsession=%3ajwcwYVVOIPYyCTPL%2c925a9db2a63a711fff5add32cfcedd8f; HttpOnly; path=/;
 port=2083; secure
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2083; secure
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=connectedpakistan.pk; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2083; secure
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 37488

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

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 v3.0 Base Score

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

VPR Score

1.4

EPSS Score

0.0307

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

1.9 (CVSS2#E:U/RL:OF/RC:C)

References

BID	32319
CVE	CVE-2008-5161
XREF	CERT:958563
XREF	CWE:200

Plugin Information

Published: 2013/10/28, Modified: 2023/10/27

Plugin Output

tcp/22/ssh

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

  aes128-cbc
  aes256-cbc

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

  aes128-cbc
  aes256-cbc
```

153953 - SSH Weak Key Exchange Algorithms Enabled

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) RFC9142. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

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

See Also

https://datatracker.ietf.org/doc/html/rfc9142

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2021/10/13, Modified: 2024/03/22

Plugin Output

tcp/22/ssh

```
The following weak key exchange algorithms are enabled :

  diffie-hellman-group-exchange-sha1
```

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/ssh

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

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: 2025/04/15

Plugin Output

tcp/0

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

  cpe:/o:linux:linux_kernel -> Linux Kernel

Following application CPE's matched on the remote system :

  cpe:/a:isc:bind:9.11.36-redhat-9.11.36-16.el8_10.4 -> ISC BIND
  cpe:/a:isc:bind:9.11.36:RedHat -> ISC BIND
  cpe:/a:openbsd:openssh:8.0 -> OpenBSD OpenSSH
```

10028 - DNS Server BIND version Directive Remote Version Detection

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 IAVT:0001-T-0583

Plugin Information

Published: 1999/10/12, Modified: 2022/10/12

Plugin Output

udp/53/dns

```
Version : 9.11.36-RedHat-9.11.36-16.el8_10.4
```

11002 - DNS Server Detection

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/dns

11002 - DNS Server Detection

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

udp/53/dns

72779 - DNS Server Version Detection

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

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0937

Plugin Information

Published: 2014/03/03, Modified: 2024/09/24

Plugin Output

tcp/53/dns

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

  9.11.36-RedHat-9.11.36-16.el8_10.4
```

35371 - DNS Server hostname.bind Map Hostname Disclosure

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/dns

```
The remote host name is :

server.domaincontrol.pk
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2025/03/12

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 65
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

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

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0943

Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :

220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 3 of 50 allowed.
220-Local time is now 17:34. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
```

42149 - FTP Service AUTH TLS Command Support

Synopsis

The remote directory service supports encrypting traffic.

Description

The remote FTP service supports the use of the 'AUTH TLS' command to switch from a cleartext to an encrypted communications channel.

See Also

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

https://tools.ietf.org/html/rfc4217

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/15, Modified: 2024/01/16

Plugin Output

tcp/21/ftp

```
The remote FTP service responded to the 'AUTH TLS' command with a
'234' response code, suggesting that it supports that command.  However,
Nessus failed to negotiate a TLS connection or get the associated SSL
certificate, perhaps because of a network connectivity problem or the
service requires a peer certificate as part of the negotiation.
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

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: 2024/08/09

Plugin Output

tcp/443/www

```
HTTP/1.1 200 OK
Connection: close
cache-control: no-cache
wpo-cache-status: cached
last-modified: Wed, 16 Jul 2025 06:53:11 GMT
content-type: text/html; charset=UTF-8
transfer-encoding: chunked
date: Wed, 16 Jul 2025 12:37:35 GMT
vary: User-Agent
alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-
Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"

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

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

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: 2024/08/09

Plugin Output

tcp/2083/www

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset="utf-8"
Date: Wed, 16 Jul 2025 12:37:36 GMT
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
Set-Cookie: cpsession=%3ajwcwYVVOIPYyCTPL%2c925a9db2a63a711fff5add32cfcedd8f; HttpOnly; path=/;
 port=2083; secure
Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2083; secure
Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=connectedpakistan.pk; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2083; secure
Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Length: 37488

The remote HTTPS server does not send the HTTP
```

```
"Strict-Transport-Security" header.
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2025/03/13

Plugin Output

tcp/0

```
5.9.177.100 resolves as ehostpk.net.
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is 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: 2024/02/26

Plugin Output

tcp/2083/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Wed, 16 Jul 2025 12:44:58 GMT
  Cache-Control: no-cache, no-store, must-revalidate, private
  Pragma: no-cache
  Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
  Set-Cookie: cpsession=%3aBqGCml6xxdIeITnH%2ca38b6d53d596cb1e435c8d228fc9ce06; HttpOnly; path=/;
 port=2083; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2083; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=connectedpakistan.pk; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
  X-Frame-Options: SAMEORIGIN
  X-Content-Type-Options: nosniff
```

```
  Content-Length: 37488

Response Body :


<!DOCTYPE html>
<html lang="en" dir="ltr">
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-
scalable=1">
    <meta name="google" content="notranslate" />
    <meta name="apple-itunes-app" content="app-id=1188352635" />
    <title>cPanel Login</title>
    <link rel="shortcut icon" href="
DfOzdnjIKFkECIVWIKvUFsIkRExa9KJCLaWAgWJx4DilZWgpDDiI0wiViIoGATP1CCEDYHSeCwUBBkgiiKURQJFiLo4d0eOxYzC8nsO9m9XcXC
+8MW+3z+9/l6l2383xH+iSBpElyTdoda26xsDqp/
h0CVZ3vwKm7tMBngAs7h7eRYebG6hMtMBHbMBX89vfARHprQ5U8cwdFQlIOZCVR5di1+w/wWXT/
EY6EoN5NZCODuKZLDwzgSMCuBe2fwfX6QZwtpWzqfBBtLC3txF/
ZhxKbBGx0EfsTJS77vwmGjlZrD4mUzUOXZjVjGI65cnTXchB8iupdDUb7QinsQZ7GzZftdQj2JVZ49iC/
w6JjksIo7OnS9tiA5Vn6GtyK2+1MY5NkhfGDygVrBAxH5WkPuMjR7/3UsUFL12Q68s4XkA3ws3v9zoSjX28Kr5wL [...]
```

11414 - IMAP Service Banner Retrieval

Synopsis

An IMAP server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/03/18, Modified: 2011/03/16

Plugin Output

tcp/143/imap

```
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS
 AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
```

11414 - IMAP Service Banner Retrieval

Synopsis

An IMAP server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/03/18, Modified: 2011/03/16

Plugin Output

tcp/993/imap

```
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ AUTH=PLAIN
 AUTH=LOGIN] Dovecot ready.
```

42085 - IMAP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote IMAP 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/rfc2595

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2021/02/24

Plugin Output

tcp/143/imap

```
The remote IMAP service responded to the 'STARTTLS' command with an
'OK' response code, suggesting that it supports that command. However,
Nessus failed to negotiate a TLS connection or get the associated SSL
certificate, perhaps because of a network connectivity problem or the
service requires a peer certificate as part of the negotiation.
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/21/ftp

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/22/ssh

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/53/dns

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/80/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/110/pop3

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/143/imap

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/443/www

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/993/imap

```
Port 993/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/995/pop3

```
Port 995/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/2077

```
Port 2077/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/2083/www

```
Port 2083/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/2086

```
Port 2086/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/8889

```
Port 8889/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- 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: 2025/06/25

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.9.0
Nessus build : 20144
Plugin feed version : 202507090133
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Advanced Scan Connected Pakistan
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.122.224
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 177.531 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 256
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/7/16 17:32 PKT (UTC +05:00)
Scan duration : 2857 sec
Scan for malware : no
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, “OS Identification”, the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Ubuntu 16.04 Linux Kernel 4.4
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
   P1:B10113:F0x12:W29200:O0204ffff:M1412:
   P2:B10113:F0x12:W28960:O0204ffff0402080affffffff4445414401030307:M1412:
   P3:B00000:F0x00:W0:O0:M0
   P4:191300_7_p=443R

Following fingerprints could not be used to determine OS :
 SSH:!:SSH-2.0-OpenSSH_8.0
SSLcert:!:i/CN:R10i/O:Let's Encrypts/CN:connectedpakistan.pk
1c9467819328d2eb1336497b4524015257f10f24
i/CN:R10i/O:Let's Encrypts/CN:connectedpakistan.pk
1c9467819328d2eb1336497b4524015257f10f24
i/CN:R10i/O:Let's Encrypts/CN:connectedpakistan.pk
1c9467819328d2eb1336497b4524015257f10f24
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2025/06/03

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP


The remote host is running Linux Kernel 2.6
```

117886 - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
    Message     :
Credentials were not provided for detected SSH service.
```

181418 - OpenSSH Detection

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

https://www.openssh.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2025/07/01

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 8.0
Banner  : SSH-2.0-OpenSSH_8.0
```

10185 - POP Server Detection

Synopsis

A POP server is listening on the remote port.

Description

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

See Also

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

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

tcp/110/pop3

```
Remote POP server banner :

+OK Dovecot ready.
```

10185 - POP Server Detection

Synopsis

A POP server is listening on the remote port.

Description

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

See Also

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

Solution

Disable this service if you do not use it.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2019/11/22

Plugin Output

tcp/995/pop3

```
Remote POP server banner :

+OK Dovecot ready.
```

42087 - POP3 Service STLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote POP3 service supports the use of the 'STLS' command to switch from a cleartext to an encrypted communications channel.

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2021/02/24

Plugin Output

tcp/110/pop3

```
The remote POP3 service responded to the 'STLS' command with an
'+OK' response code, suggesting that it supports that command. However,
Nessus failed to negotiate a TLS connection or get the associated SSL
certificate, perhaps because of a network connectivity problem or the
service requires a peer certificate as part of the negotiation.
```

31422 - Reverse NAT/Intercepting Proxy Detection

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: 2022/04/11

Plugin Output

tcp/0

```
+ On the following port(s) :
 - 21 (10 hops away)

The operating system was identified as :

FortiOS on Fortinet FortiGate

+ On the following port(s) :
 - 110 (10 hops away)
 - 80 (10 hops away)
 - 2086 (10 hops away)
 - 143 (10 hops away)
 - 995 (10 hops away)
 - 22 (10 hops away)
 - 8889 (10 hops away)
 - 53 (10 hops away)
```

```
  - 443 (10 hops away)
  - 993 (10 hops away)
  - 2083 (10 hops away)
  - 2077 (10 hops away)

The operating system was identified as :

Linux Kernel 2.6
```

70657 - SSH Algorithms and Languages Supported

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: 2025/01/20

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm(s) with the server :

  Client to Server: aes256-ctr
  Server to Client: aes256-ctr

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@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

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-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@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

The server supports the following options for kex_algorithms :

  curve25519-sha256
  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha1
  diffie-hellman-group14-sha256
  diffie-hellman-group16-sha512
  diffie-hellman-group18-sha512
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521
  kex-strict-s-v00@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 encryption_algorithms_server_to_client :

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

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: 2024/07/24

Plugin Output

tcp/22/ssh

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

  - 1.99
  - 2.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com
```

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

References

XREF IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_8.0
SSH supported authentication : publickey,gssapi-keyex,gssapi-with-mic
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/21/ftp

```
This port supports TLSv1.3/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/110/pop3

```
This port supports TLSv1.3/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/143/imap

```
This port supports TLSv1.3/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/443/www

```
This port supports TLSv1.3/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/993/imap

```
This port supports TLSv1.3/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/995/pop3

```
This port supports TLSv1.3/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2025/06/16

Plugin Output

tcp/2083/www

```
This port supports TLSv1.3/TLSv1.2.
```

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: 2021/03/09

Plugin Output

tcp/21/ftp

```
The host name known by Nessus is :

  connectedpakistan.pk

The Common Name in the certificate is :

  server.domaincontrol.pk

The Subject Alternate Names in the certificate are :

  server.domaincontrol.pk
  www.server.domaincontrol.pk
```

83298 - SSL Certificate Chain Contains Certificates Expiring Soon

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

Plugin Output

tcp/110/pop3

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject   : CN=connectedpakistan.pk
|-Not After : Aug 27 16:54:18 2025 GMT
```

83298 - SSL Certificate Chain Contains Certificates Expiring Soon

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

Plugin Output

tcp/143/imap

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject   : CN=connectedpakistan.pk
|-Not After : Aug 27 16:54:18 2025 GMT
```

83298 - SSL Certificate Chain Contains Certificates Expiring Soon

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

Plugin Output

tcp/993/imap

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject   : CN=connectedpakistan.pk
|-Not After : Aug 27 16:54:18 2025 GMT
```

83298 - SSL Certificate Chain Contains Certificates Expiring Soon

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

Plugin Output

tcp/995/pop3

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject   : CN=connectedpakistan.pk
|-Not After : Aug 27 16:54:18 2025 GMT
```

83298 - SSL Certificate Chain Contains Certificates Expiring Soon

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

Plugin Output

tcp/2083/www

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject   : CN=connectedpakistan.pk
|-Not After : Aug 27 16:54:18 2025 GMT
```

42981 - SSL Certificate Expiry - Future Expiry

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

Solution

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

Risk Factor

None

Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

Plugin Output

tcp/110/pop3

```
The SSL certificate will expire within 60 days, at
Aug 27 16:54:18 2025 GMT :

  Subject          : CN=connectedpakistan.pk
  Issuer           : C=US, O=Let's Encrypt, CN=R10
  Not valid before : May 29 16:54:19 2025 GMT
  Not valid after  : Aug 27 16:54:18 2025 GMT
```

42981 - SSL Certificate Expiry - Future Expiry

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

Solution

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

Risk Factor

None

Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

Plugin Output

tcp/143/imap

```
The SSL certificate will expire within 60 days, at
Aug 27 16:54:18 2025 GMT :

  Subject          : CN=connectedpakistan.pk
  Issuer           : C=US, O=Let's Encrypt, CN=R10
  Not valid before : May 29 16:54:19 2025 GMT
  Not valid after  : Aug 27 16:54:18 2025 GMT
```

42981 - SSL Certificate Expiry - Future Expiry

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

Solution

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

Risk Factor

None

Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

Plugin Output

tcp/993/imap

```
The SSL certificate will expire within 60 days, at
Aug 27 16:54:18 2025 GMT :

  Subject          : CN=connectedpakistan.pk
  Issuer           : C=US, O=Let's Encrypt, CN=R10
  Not valid before : May 29 16:54:19 2025 GMT
  Not valid after  : Aug 27 16:54:18 2025 GMT
```

42981 - SSL Certificate Expiry - Future Expiry

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

Solution

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

Risk Factor

None

Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

Plugin Output

tcp/995/pop3

```
The SSL certificate will expire within 60 days, at
Aug 27 16:54:18 2025 GMT :

  Subject          : CN=connectedpakistan.pk
  Issuer           : C=US, O=Let's Encrypt, CN=R10
  Not valid before : May 29 16:54:19 2025 GMT
  Not valid after  : Aug 27 16:54:18 2025 GMT
```

42981 - SSL Certificate Expiry - Future Expiry

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

Solution

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

Risk Factor

None

Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

Plugin Output

tcp/2083/www

```
The SSL certificate will expire within 60 days, at
Aug 27 16:54:18 2025 GMT :

  Subject          : CN=connectedpakistan.pk
  Issuer           : C=US, O=Let's Encrypt, CN=R10
  Not valid before : May 29 16:54:19 2025 GMT
  Not valid after  : Aug 27 16:54:18 2025 GMT
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/21/ftp

```
Subject Name:

Common Name: server.domaincontrol.pk

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 76 9A F9 61 F2 D8 4A 66 DC EB 94 4B 05 8C 47 B5

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: May 13 00:00:00 2025 GMT
Not Valid After: May 26 23:59:59 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 8B E2 6E B8 E0 37 A3 9D CB 11 7E 26 8E 88 80 45 A0 0E 84
            4F A2 52 E2 B2 63 79 8D 3C 3C 67 F9 A6 15 7D 9C BB 3D 09 99
            7E 50 BE 89 60 65 6B 32 2B B8 D2 74 52 FF 62 D1 DA 81 F2 F8
            21 B0 78 37 CA B9 B6 D3 A4 D5 82 C6 9D 6A 6C 31 F3 4E 20 39
            CD FA AC B5 3E 20 76 95 55 12 79 B2 3C 88 DC A1 74 C4 E1 A5
            01 2A 5D BB A4 84 32 EC 3C A4 03 B3 09 CA FC B4 1E DB 89 F3
            E3 D5 04 BD 72 BF 6C 56 82 2D 16 C2 42 7A 81 93 FA E3 10 67
```

```
             9F 18 2E CF CD 2A 91 DA 89 75 29 C6 9A 96 99 FC 34 CF 08 ED
             3C 8E 00 3D 99 CA 48 F5 C9 8C 80 59 E6 E7 53 DD B8 9B CD 92
             44 98 1F A0 DC 52 72 ED AF 15 D6 97 DB 73 AD DA 79 C5 A2 6B
             20 3B 1A 0B F5 3E 18 DB 88 1B 2C A5 CD 79 E3 EB 19 B1 6C 99
             23 00 72 FC DF D6 76 FF 54 24 7B AD 72 50 E9 D7 0B E2 7D 54
             65 16 18 CB B9 96 3D 52 BC 30 0B 8D 09 01 D2 AD A3
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 54 F0 B2 59 57 A4 70 56 F0 70 C9 01 D0 0A C0 B0 92 C4 D6
           12 29 08 FB 8C 08 B3 C7 C2 36 D8 19 10 39 93 83 7A 66 96 5D
           2F 66 88 95 69 D1 6B ED C8 F1 DA 45 72 B4 83 BD 55 DE 59 79
           70 63 3B B3 9D 82 97 D5 C9 B8 5D 7D 9E 25 76 95 30 D9 06 A0
           77 AD 0C DB 91 C4 4A BC 75 0D BC 38 28 15 FE 78 53 FC B1 BE
           20 50 C9 60 EE 6A 1D A6 B0 C1 C1 27 EB BA 30 FC 6A 66 FE 99
           73 BD 92 9D 64 CE 42 62 B8 B7 A7 FF 9E 2E 1B 8A 08 78 14 E1
           B6 47 A4 F4 49 94 39 37 C6 F [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/110/pop3

```
Subject Name:

Common Name: connectedpakistan.pk

Issuer Name:

Country: US
Organization: Let's Encrypt
Common Name: R10

Serial Number: 05 46 5A FE 26 DF 12 AA 8B A5 D2 04 FB DE 99 3F 78 DE

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: May 29 16:54:19 2025 GMT
Not Valid After: Aug 27 16:54:18 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 AF 42 28 51 9D EA 45 30 75 CE FA 8F C1 C3 31 13 2B 61 09
            F8 9E BB 65 99 14 33 C9 E8 E0 EB DF E7 D9 47 FD 34 AA 2E 3E
            D8 D7 46 FA EC 83 0B AB 7B 17 7E 48 7B E5 6D 53 C5 E2 07 AA
            7C F5 A4 23 2A A5 FE 3D 03 58 EC 32 FF AD 04 90 DA 3B 6A 50
            19 07 8C 52 B4 BC 88 A6 32 F7 B8 C7 D4 BD FA 1B 48 FE C3 27
            08 13 FF C7 82 79 1A 64 59 B3 99 BB 87 BC 81 1A 41 9E 60 AE
            51 9D AC BB 39 1E 51 CA A1 9E E1 96 5F DF 05 12 4B 52 B2 A8
            53 15 54 98 59 30 63 1B 41 99 2C AC B9 46 C5 03 73 D5 E3 8A
            F0 86 EB 3D 57 3D E6 7E F6 CE C8 0E F0 10 41 28 B0 D8 70 E9
```

```
            5E CA DC A0 B4 B8 E3 52 46 49 BA C8 EC CA 0C 0B F9 CA 36 89
            06 76 6B 26 23 03 CC FF 87 C9 E6 E4 E4 4F 3E 83 29 5E F5 80
            8F 00 8F 9B 2C AB 07 E8 69 F5 59 CC 4B E5 92 81 88 51 BB 83
            C6 7D 95 27 1C EA 4C 24 0B 5D A5 23 52 AE A0 45 E3
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 28 F9 BA 48 8D DD 40 F8 56 A9 F3 9A 6E CB 55 70 9D A0 59
           C3 9F 69 22 F1 AB 42 17 84 A0 65 92 11 22 9F C8 07 E2 34 42
           4F 45 9F 0A 6B F0 BC 3C FE 41 76 B7 69 53 D1 52 87 B2 B8 A4
           70 F9 83 ED E4 3A 1B E1 5B 14 AF D5 E3 B7 CB 43 68 99 ED 24
           9C B0 3E 7C C6 18 90 48 5E CD 1B 8B B5 E4 DB 47 E5 58 5D 08
           E0 4B D2 8B 49 6D 22 3D 25 0C EC 15 5A 31 AB C6 98 A3 98 F3
           0A FC 13 26 29 43 68 2B 35 39 A5 11 E8 29 6F 50 81 45 27 6C
           BB 23 77 BF 66 19 FC 30 6F 51 A2 16 17 24 F9 1B 92 91 71 D3
           75 1A 77 0A 3F 44 12 96 5D 73 26 0A D9 55 5E 89 B6  [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/143/imap

```
Subject Name:

Common Name: connectedpakistan.pk

Issuer Name:

Country: US
Organization: Let's Encrypt
Common Name: R10

Serial Number: 05 46 5A FE 26 DF 12 AA 8B A5 D2 04 FB DE 99 3F 78 DE

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: May 29 16:54:19 2025 GMT
Not Valid After: Aug 27 16:54:18 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 AF 42 28 51 9D EA 45 30 75 CE FA 8F C1 C3 31 13 2B 61 09
            F8 9E BB 65 99 14 33 C9 E8 E0 EB DF E7 D9 47 FD 34 AA 2E 3E
            D8 D7 46 FA EC 83 0B AB 7B 17 7E 48 7B E5 6D 53 C5 E2 07 AA
            7C F5 A4 23 2A A5 FE 3D 03 58 EC 32 FF AD 04 90 DA 3B 6A 50
            19 07 8C 52 B4 BC 88 A6 32 F7 B8 C7 D4 BD FA 1B 48 FE C3 27
            08 13 FF C7 82 79 1A 64 59 B3 99 BB 87 BC 81 1A 41 9E 60 AE
            51 9D AC BB 39 1E 51 CA A1 9E E1 96 5F DF 05 12 4B 52 B2 A8
            53 15 54 98 59 30 63 1B 41 99 2C AC B9 46 C5 03 73 D5 E3 8A
            F0 86 EB 3D 57 3D E6 7E F6 CE C8 0E F0 10 41 28 B0 D8 70 E9
```

```
            5E CA DC A0 B4 B8 E3 52 46 49 BA C8 EC CA 0C 0B F9 CA 36 89
            06 76 6B 26 23 03 CC FF 87 C9 E6 E4 E4 4F 3E 83 29 5E F5 80
            8F 00 8F 9B 2C AB 07 E8 69 F5 59 CC 4B E5 92 81 88 51 BB 83
            C6 7D 95 27 1C EA 4C 24 0B 5D A5 23 52 AE A0 45 E3
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 28 F9 BA 48 8D DD 40 F8 56 A9 F3 9A 6E CB 55 70 9D A0 59
           C3 9F 69 22 F1 AB 42 17 84 A0 65 92 11 22 9F C8 07 E2 34 42
           4F 45 9F 0A 6B F0 BC 3C FE 41 76 B7 69 53 D1 52 87 B2 B8 A4
           70 F9 83 ED E4 3A 1B E1 5B 14 AF D5 E3 B7 CB 43 68 99 ED 24
           9C B0 3E 7C C6 18 90 48 5E CD 1B 8B B5 E4 DB 47 E5 58 5D 08
           E0 4B D2 8B 49 6D 22 3D 25 0C EC 15 5A 31 AB C6 98 A3 98 F3
           0A FC 13 26 29 43 68 2B 35 39 A5 11 E8 29 6F 50 81 45 27 6C
           BB 23 77 BF 66 19 FC 30 6F 51 A2 16 17 24 F9 1B 92 91 71 D3
           75 1A 77 0A 3F 44 12 96 5D 73 26 0A D9 55 5E 89 B6  [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/993/imap

```
Subject Name:

Common Name: connectedpakistan.pk

Issuer Name:

Country: US
Organization: Let's Encrypt
Common Name: R10

Serial Number: 05 46 5A FE 26 DF 12 AA 8B A5 D2 04 FB DE 99 3F 78 DE

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: May 29 16:54:19 2025 GMT
Not Valid After: Aug 27 16:54:18 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 AF 42 28 51 9D EA 45 30 75 CE FA 8F C1 C3 31 13 2B 61 09
            F8 9E BB 65 99 14 33 C9 E8 E0 EB DF E7 D9 47 FD 34 AA 2E 3E
            D8 D7 46 FA EC 83 0B AB 7B 17 7E 48 7B E5 6D 53 C5 E2 07 AA
            7C F5 A4 23 2A A5 FE 3D 03 58 EC 32 FF AD 04 90 DA 3B 6A 50
            19 07 8C 52 B4 BC 88 A6 32 F7 B8 C7 D4 BD FA 1B 48 FE C3 27
            08 13 FF C7 82 79 1A 64 59 B3 99 BB 87 BC 81 1A 41 9E 60 AE
            51 9D AC BB 39 1E 51 CA A1 9E E1 96 5F DF 05 12 4B 52 B2 A8
            53 15 54 98 59 30 63 1B 41 99 2C AC B9 46 C5 03 73 D5 E3 8A
            F0 86 EB 3D 57 3D E6 7E F6 CE C8 0E F0 10 41 28 B0 D8 70 E9
```

```
             5E CA DC A0 B4 B8 E3 52 46 49 BA C8 EC CA 0C 0B F9 CA 36 89
             06 76 6B 26 23 03 CC FF 87 C9 E6 E4 E4 4F 3E 83 29 5E F5 80
             8F 00 8F 9B 2C AB 07 E8 69 F5 59 CC 4B E5 92 81 88 51 BB 83
             C6 7D 95 27 1C EA 4C 24 0B 5D A5 23 52 AE A0 45 E3
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 28 F9 BA 48 8D DD 40 F8 56 A9 F3 9A 6E CB 55 70 9D A0 59
           C3 9F 69 22 F1 AB 42 17 84 A0 65 92 11 22 9F C8 07 E2 34 42
           4F 45 9F 0A 6B F0 BC 3C FE 41 76 B7 69 53 D1 52 87 B2 B8 A4
           70 F9 83 ED E4 3A 1B E1 5B 14 AF D5 E3 B7 CB 43 68 99 ED 24
           9C B0 3E 7C C6 18 90 48 5E CD 1B 8B B5 E4 DB 47 E5 58 5D 08
           E0 4B D2 8B 49 6D 22 3D 25 0C EC 15 5A 31 AB C6 98 A3 98 F3
           0A FC 13 26 29 43 68 2B 35 39 A5 11 E8 29 6F 50 81 45 27 6C
           BB 23 77 BF 66 19 FC 30 6F 51 A2 16 17 24 F9 1B 92 91 71 D3
           75 1A 77 0A 3F 44 12 96 5D 73 26 0A D9 55 5E 89 B6  [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/995/pop3

```
Subject Name:

Common Name: connectedpakistan.pk

Issuer Name:

Country: US
Organization: Let's Encrypt
Common Name: R10

Serial Number: 05 46 5A FE 26 DF 12 AA 8B A5 D2 04 FB DE 99 3F 78 DE

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: May 29 16:54:19 2025 GMT
Not Valid After: Aug 27 16:54:18 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 AF 42 28 51 9D EA 45 30 75 CE FA 8F C1 C3 31 13 2B 61 09
            F8 9E BB 65 99 14 33 C9 E8 E0 EB DF E7 D9 47 FD 34 AA 2E 3E
            D8 D7 46 FA EC 83 0B AB 7B 17 7E 48 7B E5 6D 53 C5 E2 07 AA
            7C F5 A4 23 2A A5 FE 3D 03 58 EC 32 FF AD 04 90 DA 3B 6A 50
            19 07 8C 52 B4 BC 88 A6 32 F7 B8 C7 D4 BD FA 1B 48 FE C3 27
            08 13 FF C7 82 79 1A 64 59 B3 99 BB 87 BC 81 1A 41 9E 60 AE
            51 9D AC BB 39 1E 51 CA A1 9E E1 96 5F DF 05 12 4B 52 B2 A8
            53 15 54 98 59 30 63 1B 41 99 2C AC B9 46 C5 03 73 D5 E3 8A
            F0 86 EB 3D 57 3D E6 7E F6 CE C8 0E F0 10 41 28 B0 D8 70 E9
```

```
            5E CA DC A0 B4 B8 E3 52 46 49 BA C8 EC CA 0C 0B F9 CA 36 89
            06 76 6B 26 23 03 CC FF 87 C9 E6 E4 E4 4F 3E 83 29 5E F5 80
            8F 00 8F 9B 2C AB 07 E8 69 F5 59 CC 4B E5 92 81 88 51 BB 83
            C6 7D 95 27 1C EA 4C 24 0B 5D A5 23 52 AE A0 45 E3
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 28 F9 BA 48 8D DD 40 F8 56 A9 F3 9A 6E CB 55 70 9D A0 59
           C3 9F 69 22 F1 AB 42 17 84 A0 65 92 11 22 9F C8 07 E2 34 42
           4F 45 9F 0A 6B F0 BC 3C FE 41 76 B7 69 53 D1 52 87 B2 B8 A4
           70 F9 83 ED E4 3A 1B E1 5B 14 AF D5 E3 B7 CB 43 68 99 ED 24
           9C B0 3E 7C C6 18 90 48 5E CD 1B 8B B5 E4 DB 47 E5 58 5D 08
           E0 4B D2 8B 49 6D 22 3D 25 0C EC 15 5A 31 AB C6 98 A3 98 F3
           0A FC 13 26 29 43 68 2B 35 39 A5 11 E8 29 6F 50 81 45 27 6C
           BB 23 77 BF 66 19 FC 30 6F 51 A2 16 17 24 F9 1B 92 91 71 D3
           75 1A 77 0A 3F 44 12 96 5D 73 26 0A D9 55 5E 89 B6  [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/2083/www

```
Subject Name:

Common Name: connectedpakistan.pk

Issuer Name:

Country: US
Organization: Let's Encrypt
Common Name: R10

Serial Number: 05 46 5A FE 26 DF 12 AA 8B A5 D2 04 FB DE 99 3F 78 DE

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: May 29 16:54:19 2025 GMT
Not Valid After: Aug 27 16:54:18 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 AF 42 28 51 9D EA 45 30 75 CE FA 8F C1 C3 31 13 2B 61 09
            F8 9E BB 65 99 14 33 C9 E8 E0 EB DF E7 D9 47 FD 34 AA 2E 3E
            D8 D7 46 FA EC 83 0B AB 7B 17 7E 48 7B E5 6D 53 C5 E2 07 AA
            7C F5 A4 23 2A A5 FE 3D 03 58 EC 32 FF AD 04 90 DA 3B 6A 50
            19 07 8C 52 B4 BC 88 A6 32 F7 B8 C7 D4 BD FA 1B 48 FE C3 27
            08 13 FF C7 82 79 1A 64 59 B3 99 BB 87 BC 81 1A 41 9E 60 AE
            51 9D AC BB 39 1E 51 CA A1 9E E1 96 5F DF 05 12 4B 52 B2 A8
            53 15 54 98 59 30 63 1B 41 99 2C AC B9 46 C5 03 73 D5 E3 8A
            F0 86 EB 3D 57 3D E6 7E F6 CE C8 0E F0 10 41 28 B0 D8 70 E9
```

```
            5E CA DC A0 B4 B8 E3 52 46 49 BA C8 EC CA 0C 0B F9 CA 36 89
            06 76 6B 26 23 03 CC FF 87 C9 E6 E4 E4 4F 3E 83 29 5E F5 80
            8F 00 8F 9B 2C AB 07 E8 69 F5 59 CC 4B E5 92 81 88 51 BB 83
            C6 7D 95 27 1C EA 4C 24 0B 5D A5 23 52 AE A0 45 E3
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 28 F9 BA 48 8D DD 40 F8 56 A9 F3 9A 6E CB 55 70 9D A0 59
           C3 9F 69 22 F1 AB 42 17 84 A0 65 92 11 22 9F C8 07 E2 34 42
           4F 45 9F 0A 6B F0 BC 3C FE 41 76 B7 69 53 D1 52 87 B2 B8 A4
           70 F9 83 ED E4 3A 1B E1 5B 14 AF D5 E3 B7 CB 43 68 99 ED 24
           9C B0 3E 7C C6 18 90 48 5E CD 1B 8B B5 E4 DB 47 E5 58 5D 08
           E0 4B D2 8B 49 6D 22 3D 25 0C EC 15 5A 31 AB C6 98 A3 98 F3
           0A FC 13 26 29 43 68 2B 35 39 A5 11 E8 29 6F 50 81 45 27 6C
           BB 23 77 BF 66 19 FC 30 6F 51 A2 16 17 24 F9 1B 92 91 71 D3
           75 1A 77 0A 3F 44 12 96 5D 73 26 0A D9 55 5E 89 B6  [...]
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the 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 (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

http://www.nessus.org/u?ae636e78

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

Plugin Output

tcp/21/ftp

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

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMGh
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgc
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

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

https://www.openssl.org/docs/manmaster/man1/ciphers.html

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/21/ftp

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth      Encryption             MAC
    ----------------------        ----------        ---           ----      ---------------------  ---
    ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76        ECDH          RSA       Camellia-CBC(128)
 SHA256
    ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77        ECDH          RSA       Camellia-CBC(256)
 SHA384
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA       AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA       AES-CBC(256)
 SHA1
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45        DH            RSA       Camellia-CBC(128)
 SHA1
```

```
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH           RSA      Camellia-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH         RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH         RSA      AES-CBC(256)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA          RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA          RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA               0x00, 0x41       RSA          RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA               0x00, 0x84       RSA          RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-AES128-SHA256         0x00, 0x67       DH           RSA      AES-CBC(128)
SHA256
   DHE-RSA-AES256-SHA256         0x00, 0x6B       DH           RSA      AES-CBC(256)
SHA256
   DHE-RSA-CAMELLIA128-SHA256    0x00, 0xBE       DH           RSA      Camellia-CBC(128)
SHA256
   DHE-RSA-CAMELLIA256-SHA256    0x00, 0xC4       DH           RSA      Camellia-CBC(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH         RSA      AES-CBC(128)     [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/21/ftp

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

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     --------------------   ---
    TLS_AES_128_CCM_SHA256        0x13, 0x04        -             -        AES-CCM(128)
 AEAD
    TLS_AES_128_GCM_SHA256        0x13, 0x01        -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02        -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03        -             -        ChaCha20-Poly1305(256)
 AEAD


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     --------------------   ---
```

```
   DHE-RSA-AES-128-CCM-AEAD      0xC0, 0x9E       DH            RSA      AES-CCM(128)
AEAD
   DHE-RSA-AES-128-CCM8-AEAD     0xC0, 0xA2       DH            RSA      AES-CCM8(128)
AEAD
   DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
SHA256
   DHE-RSA-AES-256-CCM-AEAD      0xC0, 0x9F       DH            RSA      AES-CCM(256)
AEAD
   DHE-RSA-AES-256-CCM8-AEAD     0xC0, 0xA3       DH            RSA      AES-CCM8(256)
AEAD
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
SHA384
   DHE-RSA-CHACHA20-POLY1305     0xCC, 0xAA       DH            RSA      ChaCha20-Poly1305(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76       ECDH          RSA       [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/110/pop3

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

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    TLS_AES_128_CCM_SHA256        0x13, 0x04        -             -        AES-CCM(128)
 AEAD
    TLS_AES_128_GCM_SHA256        0x13, 0x01        -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02        -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03        -             -        ChaCha20-Poly1305(256)
 AEAD


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
```

```
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
 SHA256

The fields above are :

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

Note that this service does not encrypt traffic by default but does
support upgrading to an encrypted connection using STARTTLS.
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/143/imap

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

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    TLS_AES_128_CCM_SHA256        0x13, 0x04        -             -        AES-CCM(128)
 AEAD
    TLS_AES_128_GCM_SHA256        0x13, 0x01        -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02        -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03        -             -        ChaCha20-Poly1305(256)
 AEAD


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
```

```
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
 SHA256

The fields above are :

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

Note that this service does not encrypt traffic by default but does
support upgrading to an encrypted connection using STARTTLS.
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/443/www

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

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    TLS_AES_128_GCM_SHA256        0x13, 0x01        -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02        -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03        -             -        ChaCha20-Poly1305(256)
 AEAD


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
```

```
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
 SHA256

The fields above are :

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

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/993/imap

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

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     --------------------   ---
    TLS_AES_128_CCM_SHA256        0x13, 0x04        -             -        AES-CCM(128)
 AEAD
    TLS_AES_128_GCM_SHA256        0x13, 0x01        -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02        -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03        -             -        ChaCha20-Poly1305(256)
 AEAD


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     --------------------   ---
```

```
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
 SHA256

The fields above are :

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

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/995/pop3

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

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    TLS_AES_128_CCM_SHA256        0x13, 0x04        -             -        AES-CCM(128)
 AEAD
    TLS_AES_128_GCM_SHA256        0x13, 0x01        -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02        -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03        -             -        ChaCha20-Poly1305(256)
 AEAD


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
```

```
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
 SHA256

The fields above are :

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

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

Plugin Output

tcp/2083/www

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

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     --------------------   ---
    TLS_AES_128_CCM_SHA256        0x13, 0x04        -             -        AES-CCM(128)
 AEAD
    TLS_AES_128_GCM_SHA256        0x13, 0x01        -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02        -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03        -             -        ChaCha20-Poly1305(256)
 AEAD


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     --------------------   ---
```

```
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
 SHA256

The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

https://www.openssl.org/docs/manmaster/man1/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: 2021/03/09

Plugin Output

tcp/21/ftp

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth      Encryption             MAC
    ----------------------        ----------        ---           ----      ---------------------  ---
    DHE-RSA-AES-128-CCM-AEAD      0xC0, 0x9E        DH            RSA       AES-CCM(128)
 AEAD
    DHE-RSA-AES-128-CCM8-AEAD     0xC0, 0xA2        DH            RSA       AES-CCM8(128)
 AEAD
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA       AES-GCM(128)
 SHA256
    DHE-RSA-AES-256-CCM-AEAD      0xC0, 0x9F        DH            RSA       AES-CCM(256)
 AEAD
    DHE-RSA-AES-256-CCM8-AEAD     0xC0, 0xA3        DH            RSA       AES-CCM8(256)
 AEAD
```

```
   DHE-RSA-AES256-SHA384         0x00, 0x9F      DH          RSA      AES-GCM(256)
SHA384
   DHE-RSA-CHACHA20-POLY1305     0xCC, 0xAA      DH          RSA      ChaCha20-Poly1305(256)
SHA256
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F      ECDH        RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30      ECDH        RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76      ECDH        RSA      Camellia-CBC(128)
SHA256
   ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77      ECDH        RSA      Camellia-CBC(256)
SHA384
   ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8      ECDH        RSA      ChaCha20-Poly1305(256)
SHA256
   DHE-RSA-AES128-SHA            0x00, 0x33      DH          RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39      DH          RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45      DH          RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88      DH          RSA      Camellia-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13      ECDH        RSA      AES-CBC(128) [...]
```

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

https://www.openssl.org/docs/manmaster/man1/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: 2021/03/09

Plugin Output

tcp/110/pop3

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth      Encryption              MAC
    ----------------------        ----------        ---           ----      ---------------------   ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA       AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA       AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA       AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA       AES-GCM(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8        ECDH          RSA       ChaCha20-Poly1305(256)
 SHA256
```

```
The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

https://www.openssl.org/docs/manmaster/man1/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: 2021/03/09

Plugin Output

tcp/143/imap

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth      Encryption              MAC
    ----------------------        ----------        ---           ----      ---------------------   ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA       AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA       AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA       AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA       AES-GCM(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8        ECDH          RSA       ChaCha20-Poly1305(256)
 SHA256
```

```
The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

https://www.openssl.org/docs/manmaster/man1/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: 2021/03/09

Plugin Output

tcp/443/www

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth      Encryption              MAC
    ----------------------        ----------        ---           ----      ---------------------   ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA       AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA       AES-GCM(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8        ECDH          RSA       ChaCha20-Poly1305(256)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
```

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

https://www.openssl.org/docs/manmaster/man1/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: 2021/03/09

Plugin Output

tcp/993/imap

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth      Encryption              MAC
    ----------------------        ----------        ---           ----      ---------------------   ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA       AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA       AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA       AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA       AES-GCM(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8        ECDH          RSA       ChaCha20-Poly1305(256)
 SHA256
```

```
The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

https://www.openssl.org/docs/manmaster/man1/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: 2021/03/09

Plugin Output

tcp/995/pop3

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8        ECDH          RSA      ChaCha20-Poly1305(256)
 SHA256
```

```
The fields above are :

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

https://www.openssl.org/docs/manmaster/man1/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: 2021/03/09

Plugin Output

tcp/2083/www

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth      Encryption              MAC
    ----------------------        ----------        ---           ----      ---------------------   ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA       AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA       AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA       AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA       AES-GCM(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8        ECDH          RSA       ChaCha20-Poly1305(256)
 SHA256
```

```
The fields above are :

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

94761 - SSL Root Certification Authority Certificate Information

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://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

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: 2018/11/15

Plugin Output

tcp/21/ftp

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

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://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

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: 2018/11/15

Plugin Output

tcp/110/pop3

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/O=Internet Security Research Group/CN=ISRG Root X1
|-Issuer              : C=US/O=Internet Security Research Group/CN=ISRG Root X1
|-Valid From          : Jun 04 11:04:38 2015 GMT
|-Valid To            : Jun 04 11:04:38 2035 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

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://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

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: 2018/11/15

Plugin Output

tcp/143/imap

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/O=Internet Security Research Group/CN=ISRG Root X1
|-Issuer              : C=US/O=Internet Security Research Group/CN=ISRG Root X1
|-Valid From          : Jun 04 11:04:38 2015 GMT
|-Valid To            : Jun 04 11:04:38 2035 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

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://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

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: 2018/11/15

Plugin Output

tcp/993/imap

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/O=Internet Security Research Group/CN=ISRG Root X1
|-Issuer              : C=US/O=Internet Security Research Group/CN=ISRG Root X1
|-Valid From          : Jun 04 11:04:38 2015 GMT
|-Valid To            : Jun 04 11:04:38 2035 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

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://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

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: 2018/11/15

Plugin Output

tcp/995/pop3

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/O=Internet Security Research Group/CN=ISRG Root X1
|-Issuer              : C=US/O=Internet Security Research Group/CN=ISRG Root X1
|-Valid From          : Jun 04 11:04:38 2015 GMT
|-Valid To            : Jun 04 11:04:38 2035 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
```

94761 - SSL Root Certification Authority Certificate Information

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://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

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: 2018/11/15

Plugin Output

tcp/2083/www

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/O=Internet Security Research Group/CN=ISRG Root X1
|-Issuer              : C=US/O=Internet Security Research Group/CN=ISRG Root X1
|-Valid From          : Jun 04 11:04:38 2015 GMT
|-Valid To            : Jun 04 11:04:38 2035 GMT
|-Signature Algorithm : SHA-256 With RSA Encryption
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/21/ftp

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     --------------------    ---
    DHE-RSA-AES-128-CCM-AEAD      0xC0, 0x9E        DH            RSA      AES-CCM(128)
AEAD
    DHE-RSA-AES-128-CCM8-AEAD     0xC0, 0xA2        DH            RSA      AES-CCM8(128)
AEAD
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA      AES-GCM(128)
SHA256
    DHE-RSA-AES-256-CCM-AEAD      0xC0, 0x9F        DH            RSA      AES-CCM(256)
AEAD
    DHE-RSA-AES-256-CCM8-AEAD     0xC0, 0xA3        DH            RSA      AES-CCM8(256)
AEAD
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA      AES-GCM(256)
SHA384
    ECDHE-RSA-CAMELLIA-CBC-128    0xC0, 0x76        ECDH          RSA      Camellia-CBC(128)
SHA256
    ECDHE-RSA-CAMELLIA-CBC-256    0xC0, 0x77        ECDH          RSA      Camellia-CBC(256)
SHA384
    RSA-AES-128-CCM-AEAD          0xC0, 0x9C        RSA           RSA      AES-CCM(128)
AEAD
    RSA-AES-128-CCM8-AEAD         0xC0, 0xA0        RSA           RSA      AES-CCM8(128)
AEAD
    RSA-AES128-SHA256             0x00, 0x9C        RSA           RSA      AES-GCM(128)
SHA256
    RSA-AES-256-CCM-AEAD          0xC0, 0x9D        RSA           RSA      AES-CCM(256)
AEAD
    RSA-AES-256-CCM8-AEAD         0xC0, 0xA1        RSA           RSA      AES-CCM8(256)
AEAD
    RSA-AES256-SHA384             0x00, 0x9D        RSA           RSA      AES-GCM(256)
SHA384
    TLS_AES_128_CCM_SHA256        0x13, 0x04        -             -        AES-CCM(128)
AEAD
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA      AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH [...]
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/110/pop3

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     --------------------    ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA      AES-GCM(256)
 SHA384
    TLS_AES_128_CCM_SHA256        0x13, 0x04        -             -        AES-CCM(128)
 AEAD

The fields above are :

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

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/143/imap

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     --------------------    ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA      AES-GCM(256)
 SHA384
    TLS_AES_128_CCM_SHA256        0x13, 0x04        -             -        AES-CCM(128)
 AEAD

The fields above are :

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

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/993/imap

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    TLS_AES_128_CCM_SHA256        0x13, 0x04       -             -        AES-CCM(128)
 AEAD

The fields above are :

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

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/995/pop3

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     --------------------   ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    TLS_AES_128_CCM_SHA256        0x13, 0x04       -             -        AES-CCM(128)
 AEAD

The fields above are :

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

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:

- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256

TLSv1.2:

- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/2083/www

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     --------------------    ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA      AES-GCM(256)
 SHA384
    TLS_AES_128_CCM_SHA256        0x13, 0x04        -             -        AES-CCM(128)
 AEAD

The fields above are :

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/21/ftp

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/22/ssh

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/110/pop3

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/143/imap

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/443/www

```
A TLSv1.2 server answered on this port.
```

tcp/443/www

```
A web server is running on this port through TLSv1.2.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/993/imap

```
A TLSv1.2 server answered on this port.
```

tcp/993/imap

```
An IMAP server is running on this port through TLSv1.2.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/995/pop3

```
A POP3 server is running on this port through TLSv1.2.
```

tcp/995/pop3

```
A TLSv1.2 server answered on this port.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/2083/www

```
A TLSv1.2 server answered on this port.
```

tcp/2083/www

```
A web server is running on this port through TLSv1.2.
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2024/09/11

Plugin Output

tcp/443/www

```
http/1.1
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/21/ftp

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/110/pop3

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/143/imap

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/443/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/993/imap

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/995/pop3

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/2083/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

https://tools.ietf.org/html/rfc8446

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/21/ftp

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

https://tools.ietf.org/html/rfc8446

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/110/pop3

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

https://tools.ietf.org/html/rfc8446

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/143/imap

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

https://tools.ietf.org/html/rfc8446

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/443/www

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

https://tools.ietf.org/html/rfc8446

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/993/imap

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

https://tools.ietf.org/html/rfc8446

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/995/pop3

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

https://tools.ietf.org/html/rfc8446

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/2083/www

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2024/04/19

Plugin Output

tcp/0

```
SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.122.224 to 5.9.177.100 :
192.168.122.224
192.168.122.1
192.168.18.1
61.5.148.250
10.57.26.89
10.253.20.225
10.253.12.18
10.253.4.18
10.253.4.4
80.81.192.187
81.95.9.14
5.56.20.254
213.239.252.230
213.239.245.198
5.9.177.100

Hop Count: 14
```

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: 2022/07/26

Plugin Output

tcp/8889

```
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    : 8889
  Type    : spontaneous
  Banner :
0x00:  54 68 65 20 66 69 72 65 77 61 6C 6C 20 6F 6E 20    The firewall on
          0x10:  74 68 69 73 20 73 65 72 76 65 72 20 69 73 20 62    this server is b
          0x20:  6C 6F 63 6B 69 6E 67 20 79 6F 75 72 20 63 6F 6E    locking your con
          0x30:  6E 65 63 74 69 6F 6E 2E 20 59 6F 75 20 6E 65 65    nection. You nee
          0x40:  64 20 74 6F 20 63 6F 6E 74 61 63 74 20 74 68 65    d to contact the
          0x50:  20 73 65 72 76 65 72 20 6F 77 6E 65 72 20 6F 72     server owner or
          0x60:  20 68 6F 73 74 69 6E 67 20 70 72 6F 76 69 64 65     hosting provide
          0x70:  72 20 66 6F 72 20 66 75 72 74 68 65 72 20 69 6E    r for further in
          0x80:  66 6F 72 6D 61 74 69 6F 6E 2E 20 59 6F 75 72 20    formation. Your
          0x90:  62 6C 6F 63 6B 65 64 20 49 50 20 61 64 64 72 65    blocked IP addre
          0xA0:  73 73 20 69 73 3A 20 35 39 2E 31 30 33 2E 31 31    ss is: 59.103.11
          0xB0:  33 2E 33 34 20 54 68 69 73 20 73 65 72 76 65 72    3.34 This server
          0xC0:  27 73 20 68 6F 73 74 6E 61 6D 65 20 69 73 3A 20    's hostname is:
          0xD0:  73 65 72 76 65 72 2E 64 6F 6D 61 69 6E 63 6F 6E    server.domaincon
          0xE0:  74 72 6F 6C 2E 70 6B 20 0A                         trol.pk .
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/80/www

```
The following cookies are expired :

Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessauth
Path : /
Value : expired
Domain : connectedpakistan.pk
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/443/www

```
The following cookies are expired :

Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessauth
Path : /
Value : expired
Domain : connectedpakistan.pk
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/2083/www

```
The following cookies are expired :

Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessauth
Path : /
Value : expired
Domain : connectedpakistan.pk
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

10386 - Web Server No 404 Error Code Check

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: 2022/06/17

Plugin Output

tcp/80/www

```
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://connectedpakistan.pk/tUVQLM3Rw_zo.html
```

10386 - Web Server No 404 Error Code Check

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: 2022/06/17

Plugin Output

tcp/443/www

```
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 :

    https://connectedpakistan.pk/tUVQLM3Rw_zo.html
```

10386 - Web Server No 404 Error Code Check

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: 2022/06/17

Plugin Output

tcp/2083/www

```
The following string will be used :
TYPE="password"
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/443/www

```
Contents of robots.txt :

User-agent: *
Disallow: /*.html
Disallow: /*.shtml
Disallow: /*.htm
Disallow: /cgi-bin/
Sitemap: https://connectedpakistan.pk/sitemap.xml
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/2083/www

```
Contents of robots.txt :

User-agent: *
Disallow: /
```