Vulnerabilty Scanning & Testing Report
Provided by Internet Computing Solutions
P.O. Box 1005, Greenwood, IN 46142
For Questions regarding this report please email: us

Your Main FCU

Fri, 1 Jan 2021 11:01:45 Eastern Standard Time

TABLE OF CONTENTS

Vulnerabilities by Plugin

- 137702 (1) - Treck TCP/IP stack multiple vulnerabilities. (Ripple20)
- 35291 (1) - SSL Certificate Signed Using Weak Hashing Algorithm
- 51192 (1) - SSL Certificate Cannot Be Trusted
- 57582 (1) - SSL Self-Signed Certificate
- 22964 (3) - Service Detection
- 10335 (2) - Nessus TCP scanner
- 11219 (2) - Nessus SYN scanner
- 10107 (1) - HTTP Server Type and Version
- 10180 (1) - Ping the remote host
- 10267 (1) - SSH Server Type and Version Information
- 10287 (1) - Traceroute Information
- 10662 (1) - Web mirroring
- 10863 (1) - SSL Certificate Information
- 10881 (1) - SSH Protocol Versions Supported
- 11032 (1) - Web Server Directory Enumeration
- 11919 (1) - HMAP Web Server Fingerprinting
- 11935 (1) - IPSEC Internet Key Exchange (IKE) Version 1 Detection
- 12053 (1) - Host Fully Qualified Domain Name (FQDN) Resolution
- 14788 (1) - IP Protocols Scan
- 19506 (1) - Nessus Scan Information
- 21643 (1) - SSL Cipher Suites Supported
- 24260 (1) - HyperText Transfer Protocol (HTTP) Information
- 25220 (1) - TCP/IP Timestamps Supported
- 43111 (1) - HTTP Methods Allowed (per directory)
- 45410 (1) - SSL Certificate 'commonName' Mismatch
- 45590 (1) - Common Platform Enumeration (CPE)
- 46215 (1) - Inconsistent Hostname and IP Address
- 49704 (1) - External URLs
- 50344 (1) - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
- 50350 (1) - OS Identification Failed
- 56984 (1) - SSL / TLS Versions Supported
- 57041 (1) - SSL Perfect Forward Secrecy Cipher Suites Supported
- 66334 (1) - Patch Report
- 70544 (1) - SSL Cipher Block Chaining Cipher Suites Supported
- 70657 (1) - SSH Algorithms and Languages Supported
- 84502 (1) - HSTS Missing From HTTPS Server
- 84821 (1) - TLS ALPN Supported Protocol Enumeration
- 91634 (1) - HyperText Transfer Protocol (HTTP) Redirect Information
- 91815 (1) - Web Application Sitemap
- 94761 (1) - SSL Root Certification Authority Certificate Information
- 110723 (1) - Target Credential Status by Authentication Protocol - No Credentials Provided

- 117886 (1) - OS Security Patch Assessment Not Available
- 121010 (1) - TLS Version 1.1 Protocol Detection
- 136318 (1) - TLS Version 1.2 Protocol Detection
- 138614 (1) - Treck/Kasago Network Stack Detection
- 149334 (1) - SSH Password Authentication Accepted

Vulnerabilities by Plugin

Collapse All | Expand All

137702 (1) - Treck TCP/IP stack multiple vulnerabilities. (Ripple20) -

Synopsis

The Treck network stack used by the remote host is affected by multiple vulnerabilities.

Description

This plugin detects the usage of the Treck TCP/IP stack by the host thereby indicating that it could be potentially vulnerable to the Ripple20 vulnerabilities. Patches are being slowly rolled out by vendors and we will release plugins for patches as they are released by the vendors. In the interim, if you have applied the patches from the vendor for the Ripple20 vulnerabilities on this host, please recast the severity of this plugin.

Note: This plugin requires ICMP traffic to be unblocked between the scanner and the host

See Also

https://www.jsof-tech.com/ripple20/
http://www.nessus.org/u?431098c1
https://support.hp.com/emea_africa-en/document/c06640149
https://psirt.bosch.com/security-advisories/BOSCH-SA-662084.html

Solution

Apply the relevant patches as they become available.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

CVSS Base Score

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

CVSS Temporal Score

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

References

CVE	CVE-2020-11896
CVE	CVE-2020-11897
CVE	CVE-2020-11898
CVE	CVE-2020-11899
CVE	CVE-2020-11900
CVE	CVE-2020-11901
CVE	CVE-2020-11902
CVE	CVE-2020-11903
CVE	CVE-2020-11904
CVE	CVE-2020-11905
CVE	CVE-2020-11906
CVE	CVE-2020-11907
CVE	CVE-2020-11908
CVE	CVE-2020-11909
CVE	CVE-2020-11910
CVE	CVE-2020-11911
CVE	CVE-2020-11912
CVE	CVE-2020-11913
CVE	CVE-2020-11914

Plugin Information

Published: 2020/06/22, Modified: 2020/08/20

Plugin Output

10.1.10.11 (tcp/0)

```
Detected Treck TCP\IP network stack.
```

35291 (1) - SSL Certificate Signed Using Weak Hashing Algorithm -

Synopsis

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

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

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

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279
http://www.nessus.org/u?9bb87bf2
http://www.nessus.org/u?e120eea1
http://www.nessus.org/u?5d894816
http://www.nessus.org/u?51db68aa
http://www.nessus.org/u?9dc7bfba

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS Base Score

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

CVSS Temporal Score

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

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2009/01/05, Modified: 2020/04/27

Plugin Output

10.1.10.11 (tcp/9443)

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

|-Subject : C=US/ST=Illinois/L=Chicago/O=my Firewall Security Corporation/CN=Root CA
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From : Feb 04 02:49:20 2006 GMT
```

```
|-Valid To : Jan 30 02:49:20 2026 GMT

|-Subject : C=US/ST=Illinois/O=My Firewall Security Corporation/CN=My Firewall CA
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From : Feb 04 02:49:25 2006 GMT
|-Valid To : Jan 30 02:49:25 2026 GMT

|-Subject : C=US/ST=Illinois/O=My Firewall Security Corporation/CN=05A6 FW1000 Device CA
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From : Nov 02 16:07:43 2011 GMT
|-Valid To : Oct 30 16:07:43 2021 GMT

|-Subject : C=US/ST=Illinois/O=My Firewall Security Corporation/CN=MyFirewall
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From : Nov 02 16:07:49 2011 GMT
|-Valid To : Oct 30 16:07:49 2021 GMT
```

51192 (1) - SSL Certificate Cannot Be Trusted -

Synopsis

The SSL certificate for this service cannot be trusted.

Description

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

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

10.1.10.11 (tcp/9443)

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

|-Subject : C=US/ST=Illinois/L=Chicago/O=My Firewall Security Corporation/CN=Root CA
|-Issuer : C=US/ST=Illinois/L=Chicago/O=My Firewall Security Corporation/CN=Root CA
```

57582 (1) - SSL Self-Signed Certificate -

Synopsis

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

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

10.1.10.11 (tcp/9443)

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

|-Subject : C=US/ST=Illinois/L=Chicago/O=My Firewall Security Corporation/CN=Root CA
```

22964 (3) - 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: 2021/04/14

Plugin Output

10.1.10.11 (tcp/7022)

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

10.1.10.11 (tcp/9443)

```
A TLSv1.1 server answered on this port.
```

10.1.10.11 (tcp/9443)

```
A web server is running on this port through TLSv1.1.
```

10335 (2) - Nessus TCP scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/07/12

Plugin Output

10.1.10.11 (tcp/7022)

```
Port 7022/tcp was found to be open
```

10.1.10.11 (tcp/9443)

```
Port 9443/tcp was found to be open
```

11219 (2) - 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: 2021/07/12

Plugin Output

10.1.10.11 (tcp/7022)

```
Port 7022/tcp was found to be open
```

10.1.10.11 (tcp/9443)

```
Port 9443/tcp was found to be open
```

10107 (1) - HTTP Server Type and Version -

Synopsis

A web server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

10.1.10.11 (tcp/9443)

```
The remote web server type is :

HTTP Server
```

10180 (1) - Ping the remote host -

Synopsis

It was possible to identify the status of the remote host (alive or dead).

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/06/24, Modified: 2020/06/12

Plugin Output

10.1.10.11 (tcp/0)

```
The remote host is up
The remote host replied to an ICMP echo packet
```

10267 (1) - 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: 2020/09/22

Plugin Output

10.1.10.11 (tcp/7022)

```
SSH version : SSH-2.0-OpenSSH_8.1
SSH supported authentication : publickey,password,keyboard-interactive
```

10287 (1) - 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: 2020/08/20

Plugin Output

10.1.10.11 (udp/0)

```
For your information, here is the traceroute from 10.1.10.101 to 10.1.10.11 :
10.1.10.101
10.1.10.254
111.245.220.1
81.152.199.98
12.122.132.2
12.123.159.53
12.247.252.26
74.40.2.146
74.42.113.126
10.1.10.11

Hop Count: 9
```

10662 (1) - Web mirroring -

Synopsis

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/05/04, Modified: 2021/07/12

Plugin Output

10.1.10.11 (tcp/9443)

```
Webmirror performed 12 queries in 6s (2.000 queries per second)

The following CGIs have been discovered :


+ CGI : /v2/login.php
Methods : POST
Argument : cookie
Value: 119332649
Argument : login
Value: Login
Argument : page
Argument : password
Argument : username
```

10863 (1) - 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

10.1.10.11 (tcp/9443)

```
Subject Name:

Country: US
State/Province: Illinois
Organization: My Firewall Security Corporation
Common Name: MyFirewall

Issuer Name:

Country: US
State/Province: Illinois
Organization: My Firewall Security Corporation
Common Name: 05A6 FW1000 Device CA

Serial Number: 01

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Nov 02 16:07:49 2011 GMT
Not Valid After: Oct 30 16:07:49 2021 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B0 2B D3 CC FC 9A AF 61 49 39 11 0E 87 32 18 22 18 C1 0C
59 74 38 37 E5 C0 B1 96 2E 46 90 4C 3C F9 9A E3 80 0C B6 0F
E9 1C C6 B7 F0 E7 A5 4A 09 24 84 B5 11 36 4D BE 25 08 E6 B0
53 EE B5 5B 96 D4 60 2C 01 6E 01 B5 1D D5 AC 44 B3 DA 2F 92
AD 1A A3 DA F6 9D 07 49 31 9F 41 2D 35 D6 70 00 C9 5F 3B 44
5C FD 97 D7 1F 30 43 9D 49 07 E9 B0 ED D4 63 F4 9D F8 19 78
E3 F4 B4 FC 1A 98 A4 61 12 FE 2D 63 83 F2 BF 46 0C 14 42 A5
A3 E6 F8 81 9E 37 DB 49 23 B5 DD 1D 04 0F 29 95 D5 82 E3 73
FE 4E F9 C6 BD 71 33 02 5F C9 7A 5D F1 7E 68 0E 87 52 B0 BF
EB 98 9B FD 21 C3 27 3A BA 08 DE 9C 6F 88 B7 10 C3 22 82 C2
9B C3 46 CA 7C AB 74 61 B8 3A FE 35 3F 36 12 37 4F 87 03 C9
45 E4 E2 24 F1 62 50 7C A5 7D B3 A6 28 1C 23 A7 A5 A0 36 3B
7F 29 D7 B0 DD 58 41 87 93 0F 94 8C 08 5A C5 FD B1
Exponent: 01 00 01
```

```
Signature Length: 256 bytes / 2048 bits
Signature: 00 52 EA C4 14 DF 82 B7 E9 F2 C5 C9 17 55 95 EB 47 04 BB AE
BF 32 4F 34 96 B6 F8 23 F6 6F D6 EB 15 7C 9F E9 D4 C8 E3 CF
56 CD 18 9A D6 20 9A A3 72 45 62 87 08 1D 18 F1 B1 52 7A 72
9E 51 1C AF 5E 29 D5 46 95 85 52 4D 51 CA 22 27 9E 3D 59 AB
92 74 7C 34 9F 60 14 42 F3 9C 59 7F A8 83 26 4A 77 09 21 4D
59 5B 2D 7C BF 6A 18 02 BA 33 24 0E AD 01 33 B9 80 40 04 EA
46 43 55 84 E6 FA 3F 53 8D DE 61 B5 45 3E 22 F5 10 68 C5 E3
01 87 70 65 02 72 9F 26 41 3E 7B 0F 33 E8 1A 4D D8 5D 49 78
3F C5 FA 00 0E F2 B0 F6 55 5B 91 B2 C3 D4 20 0C 12 27 E2 98
93 F6 FB 2C E1 20 62 55 B3 19 E3 0D 8A E0 35 38 09 22 8A AB
D8 4E 83 5D 97 53 1D 84 57 07 0F F4 0E B1 84 60 77 B8 5C FB
74 C4 90 7D 6D DB 79 12 EA 83 F1 3E 9F B0 27 26 F7 F3 A5 29
23 7C 18 A6 AF 1A 60 63 36 81 AF A5 FB CB 0B 22 43

Extension: Basic Constraints (2.5.29.19)
Critical: 0


Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40


Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 3E 97 9E E8 29 35 A5 91 03 CF FB 86 61 0D CE 64 BC 12 AE D7


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 3C 57 23 8F 2D 67 0F F9 90 35 E1 CC 0A 39 7A 2A FF 77 C4 1E
Country: US
State/Province: Illinois
Organization: My Firewall Security Corporation
Common Name: MyFirewall CA
Serial Number: 05 A6


Fingerprints :

SHA-256 Fingerprint: 05 4B F8 9E 94 03 19 F8 11 63 39 68 DE 00 4B 40 2C F4 79 8B
AB 51 7B 2F 0D 55 C5 E6 19 79 63 94
SHA-1 Fingerprint: B3 03 42 3F D9 7A 8D 52 E8 C0 A8 C1 A9 67 31 61 91 20 D4 C2
MD5 Fingerprint: E1 35 49 EB 44 6B 39 76 C2 5C B3 8B 2F D5 DA 24


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIEKTCCAxGgAwIBAgIBATANBgkqhkiG9w0BAQUFADBtMQswCQYDVQQGEwJVUzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExJjAkBgNVBAoTHUNhbHlwdGl4IFNlY3VyaXR5IENvcnBvcmE
-----END CERTIFICATE-----
```

10881 (1) - 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: 2021/01/19

Plugin Output

10.1.10.11 (tcp/7022)

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

- 1.99
- 2.0
```

11032 (1) - Web Server Directory Enumeration -

Synopsis

It is possible to enumerate directories on the web server.

Description

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

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

n/a

Risk Factor

None

References

XREF OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2020/06/12

Plugin Output

10.1.10.11 (tcp/9443)

```
The following directories were discovered:
/download, /errors, /images, /updates

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

11919 (1) - HMAP Web Server Fingerprinting -

Synopsis

HMAP fingerprints the remote HTTP server.

Description

Nessus was able to identify the remote web server type by sending several valid and invalid HTTP requests. In some cases, its version can also be approximated, as well as some options.

See Also

http://www.nessus.org/u?05d4ce87
http://seclab.cs.ucdavis.edu/papers/hmap-thesis.pdf
http://projects.webappsec.org/w/page/13246925/Fingerprinting

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/11/11, Modified: 2020/06/12

Plugin Output

10.1.10.11 (tcp/9443)

```
Nessus was not able to exactly identify this server. It might be :

Apache/2.2.22 (Debian) or Apache/2.4.10 (Debian) or Apache/2.4.25 (Debian) or Apache/2.4.7 (Ubuntu)

The fingerprint differs from the known signatures on 3 point(s).

If you know what this server is and if you are using an up to date version
of this script, please send this signature to www-signatures@nessus.org :
```

```
HTM:HTM:400:200:400:400:400:400:400:400:400:404:405:405:405:405:405:200:404:::HTTP Server [R]
Including these headers :

ETag: "5dd42cc7-10e"
X-Frame-Options: SAMEORIGIN

Try to provide as much information as you can - software & operating
system release, sub-version, patch numbers, and specific configuration
options, if any.
```

11935 (1) - IPSEC Internet Key Exchange (IKE) Version 1 Detection -

Synopsis

A VPN server is listening on the remote port.

Description

The remote host seems to be enabled to do Internet Key Exchange (IKE) version 1. This is typically indicative of a VPN server. VPN servers are used to connect remote hosts into internal resources.

Make sure that the use of this VPN endpoint is done in accordance with your corporate security policy.

Note that if the remote host is not configured to allow the Nessus host to perform IKE/IPSEC negotiations, Nessus won't be able to detect the IKE service.

Also note that this plugin does not run over IPv6.

Solution

If this service is not needed, disable it or filter incoming traffic to this port.

Risk Factor

None

References

XREF IAVT:0001-T-0900

Plugin Information

Published: 2003/12/02, Modified: 2020/09/22

Plugin Output

10.1.10.11 (udp/500)

```
Nessus was able to get the following IKE vendor ID(s):
draft-ietf-ipsec-nat-t-ike-02
draft-ietf-ipsec-nat-t-ike-03
RFC 3947 NAT-T
Dead Peer Detection v1.0
```

12053 (1) - 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: 2017/04/14

Plugin Output

10.1.10.11 (tcp/0)

```
10.1.10.11 resolves as static-10-1-10-11.chi.il.comcast.net.
```

14788 (1) - IP Protocols Scan -

Synopsis

This plugin detects the protocols understood by the remote IP stack.

Description

This plugin detects the protocols understood by the remote IP stack.

See Also

http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/09/22, Modified: 2019/03/06

Plugin Output

10.1.10.11 (tcp/0)

```
The following IP protocols are accepted on this host:
1ICMP
2IGMP
4IP
6TCP
17UDP
41IPv6
47GRE
50ESP
51AH
55MOBILE
58IPv6-ICMP
97ETHERIP
112VRRP
132SCTP
137MPLS-in-IP
240
```

19506 (1) - 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: 2021/06/28

Plugin Output

10.1.10.11 (tcp/0)

```
  Information about this scan :

  Nessus version : 9.9.9
  Nessus build : 20299
  Plugin feed version : 202109999999
  Scanner OS : WINDOWS
  Scanner distribution : win-x86-64
  Scan type : Normal
  Scan policy used : All Tests
  Scanner IP : 10.1.10.101
  Port scanner(s) : nessus_syn_scanner
  Port range : all
  Ping RTT : 20.0 ms
  Thorough tests : yes
  Experimental tests : yes
  Paranoia level : 2
  Report verbosity : 2
  Safe checks : no
  Optimize the test : yes
  Credentialed checks : no
  Patch management checks : None
  Display superseded patches : yes (supersedence plugin launched)
  CGI scanning : enabled
  Web application tests : disabled
  Max hosts : 2
  Max checks : 2
  Recv timeout : 10
  Backports : None
  Allow post-scan editing: Yes
  Scan Start Date : 2021/1/1 11:01 Eastern Standard Time
  Scan duration : 6893 sec
```

21643 (1) - 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/man1.1.0/apps/ciphers.html
http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

Plugin Output

10.1.10.11 (tcp/9443)

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

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

  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
  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-CHACHA20-POLY1305 0xCC, 0xA8 ECDH RSA ChaCha20-Poly1305(256) SHA256
RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256
RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(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) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256
RSA-CAMELLIA128-SHA256 0x00, 0xBA RSA RSA Camellia-CBC(128) SHA256
RSA-CAMELLIA256-SHA256 0x00, 0xC0 RSA RSA Camellia-CBC(256) SHA256


SSL Version : TLSv11
High Strength Ciphers (>= 112-bit key)

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

The fields above are :

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

24260 (1) - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

10.1.10.11 (tcp/9443)

```
  Response Code : HTTP/1.1 200 OK

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

  Server: HTTP Server
  Date: Tue, 20 Jul 2021 03:03:15 GMT
```

```
Content-Type: text/html
Content-Length: 270
Last-Modified: Tue, 19 Nov 2019 17:56:23 GMT
Connection: keep-alive
ETag: "5dd42cc7-10e"
X-Frame-Options: SAMEORIGIN
Accept-Ranges: bytes

Response Body :

<html>
<head>
<title>Redirecting page...</title>
<meta http-equiv="refresh" content="0; url=/v2/login.php">
</head>

<body bgcolor="white">
You will be redirected to the login page now.
If nothing happens, please click <a href="/v2/login.php">here</a>.
</body>

</html>
```

25220 (1) - 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: 2019/03/06

Plugin Output

10.1.10.11 (tcp/0)

43111 (1) - HTTP Methods Allowed (per directory) -

Synopsis

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

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a
http://www.nessus.org/u?b019cbdb
https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2019/03/19

Plugin Output

10.1.10.11 (tcp/9443)

```
Based on tests of each method :

- HTTP methods GET HEAD POST are allowed on :

/
/download
/errors
/images
/updates
/v2
```

45410 (1) - 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

10.1.10.11 (tcp/9443)

```
The host name known by Nessus is :

static-10-1-10-11.chi.il.comcast.net

The Common Name in the certificate is :

myfirewall
```

45590 (1) - 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: 2021/07/12

Plugin Output

10.1.10.11 (tcp/0)

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

cpe:/a:openbsd:openssh:8.1
```

46215 (1) - Inconsistent Hostname and IP Address -

Synopsis

The remote host's hostname is not consistent with DNS information.

Description

The name of this machine either does not resolve or resolves to a different IP address.

This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host.

As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.

Solution

Fix the reverse DNS or host file.

Risk Factor

None

Plugin Information

Published: 2010/05/03, Modified: 2016/08/05

Plugin Output

10.1.10.11 (tcp/0)

```
The host name 'static-10-1-10-11.chi.il.comcast.net' does not resolve to an IP address
```

49704 (1) - External URLs -

Synopsis

Links to external sites were gathered.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

Plugin Output

10.1.10.11 (tcp/9443)

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

http://www.My Firewall.com/license/ - /v2/login.php
```

50344 (1) - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header -

Synopsis

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

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://www.nessus.org/u?55aa8f57
http://www.nessus.org/u?07cc2a06
https://content-security-policy.com/
https://www.w3.org/TR/CSP2/

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

10.1.10.11 (tcp/9443)

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

- https://10.1.10.11:9443/
- https://10.1.10.11:9443/v2/
- https://10.1.10.11:9443/v2/login.php
```

50350 (1) - OS Identification Failed -

Synopsis

It was not possible to determine the remote operating system.

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. Unfortunately, though, Nessus does not currently know how to use them to identify the overall system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2020/01/22

Plugin Output

10.1.10.11 (tcp/0)

```
If you think these signatures would help us improve OS fingerprinting,
please send them to :

os-signatures@nessus.org

Be sure to include a brief description of the device itself, such as
the actual operating system or product / model names.

HTTP:!:Server: HTTP Server
```

```
ICMP:!::1:1:1:255:0::1:0:::0::1:8:255:0:1:1:2:1:1:1:0:1:64:16384:MNNSNWNNT:6:1:1
SSLcert:!:i/CN:05A6 FW1000 Device CAi/O:My Firewall Security Corporations/CN:MyFirewalls/O:My Firewall Security
Corporation
b303423fd97a8d52e8c0a8c1a96731619120d4c2

SinFP:!:
P1:B11013:F0x12:W16384:O0204ffff:M1460:
P2:B11013:F0x12:W16384:O0204ffff010104020103030601010 80affffffff44454144:M1460:
P3:B00000:F0x00:W0:O0:M0
P4:80701_7_p=7022R
```

56984 (1) - 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: 2021/02/03

Plugin Output

10.1.10.11 (tcp/9443)

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

57041 (1) - 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

10.1.10.11 (tcp/9443)

```
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
```

```
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-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) SHA1
ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-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) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384

The fields above are :

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

66334 (1) - Patch Report -

Synopsis

The remote host is missing several patches.

Description

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

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2021/07/13

Plugin Output

10.1.10.11 (tcp/0)

```
. You need to take the following action :

[ Treck TCP/IP stack multiple vulnerabilities. (Ripple20) (137702) ]

+ Action to take : Apply the relevant patches as they become available.
```

70544 (1) - 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

10.1.10.11 (tcp/9443)

```
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
---------------------- ---------- --- ---- --------------------- ---
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) SHA256
ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384
RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256
RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256
RSA-CAMELLIA128-SHA256 0x00, 0xBA RSA RSA Camellia-CBC(128) SHA256
RSA-CAMELLIA256-SHA256 0x00, 0xC0 RSA RSA Camellia-CBC(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}
```

70657 (1) - 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: 2017/08/28

Plugin Output

10.1.10.11 (tcp/7022)

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

The server supports the following options for kex_algorithms :

curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
```

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

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

The server supports the following options for encryption_algorithms_client_to_server :

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

The server supports the following options for encryption_algorithms_server_to_client :

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

The server supports the following options for mac_algorithms_client_to_server :

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

The server supports the following options for mac_algorithms_server_to_client :

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

The server supports the following options for compression_algorithms_client_to_server :

none
zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

none
zlib@openssh.com
```

84502 (1) - 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: 2021/05/19

Plugin Output

10.1.10.11 (tcp/9443)

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

84821 (1) - 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: 2021/02/03

Plugin Output

10.1.10.11 (tcp/9443)

```
http/1.1
```

91634 (1) - HyperText Transfer Protocol (HTTP) Redirect Information -

Synopsis

The remote web server redirects requests to the root directory.

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.

This plugin is informational only and does not denote a security problem.

Solution

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

Risk Factor

None

Plugin Information

Published: 2016/06/16, Modified: 2017/10/12

Plugin Output

10.1.10.11 (tcp/9443)

```
Request : https://10.1.10.11:9443/
HTTP response : HTTP/1.1 200 OK
Redirect to : https://10.1.10.11:9443/v2/login.php
Redirect type : meta redirect

Final page : https://10.1.10.11:9443/v2/login.php
HTTP response : HTTP/1.1 200 OK
```

91815 (1) - Web Application Sitemap -

Synopsis

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

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

10.1.10.11 (tcp/9443)

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

- https://10.1.10.11:9443/
- https://10.1.10.11:9443/v2/
- https://10.1.10.11:9443/v2/login.php

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

94761 (1) - 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

10.1.10.11 (tcp/9443)

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

|-Subject : C=US/ST=Illinois/L=Chicago/O=My Firewall Security Corporation/CN=Root CA
|-Issuer : C=US/ST=Illinois/L=Chicago/O=My Firewall Security Corporation/CN=Root CA
|-Valid From : Feb 04 02:49:20 2006 GMT
|-Valid To : Jan 30 02:49:20 2026 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

110723 (1) - 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: 2021/01/25

Plugin Output

10.1.10.11 (tcp/0)

```
SSH was detected on port 7022 but no credentials were provided.
SSH local checks were not enabled.
```

117886 (1) - 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

10.1.10.11 (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.
```

121010 (1) - TLS Version 1.1 Protocol Detection -

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1.
TLS 1.1 lacks support for current and recommended cipher suites.
Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00
http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

10.1.10.11 (tcp/9443)

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

136318 (1) - 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

10.1.10.11 (tcp/9443)

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

138614 (1) - Treck/Kasago Network Stack Detection -

Synopsis

Attempts to detect the Treck network stack.

Description

The Treck/Kasago network stack appears to be running on the remote host.

Note that this plugin is based on detection methods provided by JSOF (https://www.jsof-tech.com/).

This plugin uses additional methods to detect the Treck/Kasago TCP/IP stack. These methods are known to have false positives. Every trigger of the plugin needs to be investigated manually for confirmation.

See Also

https://www.treck.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/07/20, Modified: 2021/07/12

Plugin Output

10.1.10.11 (tcp/0)

```
The remote host appears to be running the Treck/Kasago network stack.


IP TTL test :

ICMP echoreply TTL : 246
TCP RST TTL : 55
```

149334 (1) - SSH Password Authentication Accepted -

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

10.1.10.11 (tcp/7022)