Tenable Vulnerability Management Report

Tenable Vulnerability Management

Thu, 18 Dec 2025 18:28:31 UTC

Table Of Contents

Vulnerabilities By Plugin

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 v3.0 Base Score

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

CVSS Base Score

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

Plugin Information:

Publication date: 2012/01/17, Modification date: 2022/06/14

Assets

10.1.0.164 (TCP/3389) Vulnerability State: Active

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

|-Subject : CN=LogNPacific3286
```

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

CVSS Base Score

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

Plugin Information:

Publication date: 2010/12/15, Modification date: 2025/06/16

Assets

10.1.0.164 (TCP/3389) Vulnerability State: Active

```
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 : CN=LogNPacific3286
|-Issuer  : CN=LogNPacific3286
```

10114 (1) - ICMP Timestamp Request Remote Date Disclosure

Synopsis

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

Description

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

Solution

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

Risk Factor

Low

Vulnerability Priority Rating (VPR)

2.2

CVSS Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE-200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2024/10/07

Assets

10.1.0.164 (ICMP/0) Vulnerability State: Active

```
This host returns non-standard timestamps (high bit is set)
The ICMP timestamps might be in little endian format (not in network format)
The remote clock is synchronized with the local clock.
```

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:

Publication date: 2008/05/19, Modification date: 2021/02/03

Assets

10.1.0.164 (TCP/3389) Vulnerability State: Active

```
 Subject Name:

Common Name: LogNPacific3286

Issuer Name:

Common Name: LogNPacific3286

Serial Number: 1E 47 E8 36 4B 74 C3 A9 46 E5 2C 0D 58 B7 FF D5

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Dec 15 16:13:33 2025 GMT
Not Valid After: Jun 16 16:13:33 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 AD 24 55 B1 54 7E E8 51 0E 7C F0 D7 12 21 C5 54 52 50 35
            1B 41 38 B5 92 07 AB DF 29 0B BC 09 D4 BB BA 01 A9 F1 9E 96
            E5 2A A3 7E A4 14 E6 6A 4E D9 01 10 D1 95 88 EC F6 AF 5E 29
            03 71 63 9E 71 59 0B 0F F5 9B 99 93 A6 88 9B CE CC EA C4 DD
            E8 CB D1 95 DF 18 45 65 4B 12 17 D3 64 35 11 2A 0A 14 AF E0
            59 43 E9 DD 71 B4 7D D8 C8 99 40 7D C8 70 0F 36 A9 CE 01 35
            97 70 E7 61 AA EF 81 48 B4 15 22 28 FF 53 5A 42 C0 DE EA C6
            27 40 FF 7B 09 BD 76 FA 09 1B 73 A4 AC 66 D7 95 F5 E1 5D 84
            53 E9 5A F7 DD 20 7C B0 96 DF 75 06 04 1E 7B 8C 6D 0B 38 35
            98 DA 4B 5E 54 17 13 DB 6F DC 68 A9 AB F4 F0 E0 A8 40 44 09
            50 DE F9 59 28 6A B5 94 33 B1 DF FD 8A E4 04 E5 D0 18 C6 59
            8E 95 81 84 B0 BE 36 1B 27 9D AD 08 5D DC 08 93 0F 3D DD 6F
            3D 9D 5F 1F C2 69 8B D1 D5 8E 6D D9 80 6A 48 4C A1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 00 DA B8 5E E3 9C D9 6B C2 5A F0 6D 10 C0 14 4D 0E E8 4F
           FA FA 24 E2 23 E1 CE 26 71 4E 39 0F 49 77 0C B1 B7 FE 8C D1
           C7 2A E1 15 C6 FD 40 59 82 A2 68 C0 E2 9E CC 18 6C 9C 19 2A
           9D 05 7F 85 00 38 84 91 FD A5 58 84 34 F6 72 73 16 DB 9C AC
           B3 B5 DA 76 2B DF 10 F1 A7 33 19 EF 98 5E 49 C0 15 F6 D5 5C
           80 2B 8E 36 EB E2 35 0C 1E 9B 8D 69 24 3E 4D 17 D3 2A C5 AD
           EB 9C D3 15 CA 63 7D 79 36 6C BE 51 69 A0 48 E0 71 51 AE 30
           20 C9 70 87 F3 A1 8E 55 EE 41 21 BE 7C AF B1 EF D5 12 A3 DB
           20 2B 8F C3 10 E8 23 BE 7D 47 96 E3 A8 C8 70 BE FF E7 AD A4
           C8 F2 DE D1 E2 56 [...]
```

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:

Publication date: 2020/05/04, Modification date: 2020/05/04

Assets

10.1.0.164 (TCP/3389) Vulnerability State: Active

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

138330 (1) - 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:

Publication date: 2020/07/09, Modification date: 2023/12/13

Assets

10.1.0.164 (TCP/3389) Vulnerability State: Active

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

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:

Publication date: 2011/12/07, Modification date: 2021/03/09

Assets

10.1.0.164 (TCP/3389) Vulnerability State: Active

```
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       DHE           RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DHE           RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDHE         RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDHE         RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDHE         RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDHE         RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDHE         RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDHE         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}
```

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:

Publication date: 2013/10/22, Modification date: 2021/02/03

Assets

10.1.0.164 (TCP/3389) Vulnerability State: Active

```
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-AES128-SHA          0xC0, 0x13       ECDHE         RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDHE         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
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDHE         RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDHE         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

The fields above are :

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

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:

Publication date: 2007/05/16, Modification date: 2023/10/17

Assets

10.1.0.164 (TCP/0) Vulnerability State: Active

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:

Publication date: 2005/08/26, Modification date: 2025/10/29

Assets

10.1.0.164 (TCP/0) Vulnerability State: Active

```
Information about this scan :

Nessus version : 10.11.1
Nessus build : 20021
Plugin feed version : 202512161429
Scanner edition used : Nessus
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Win11_DISASTIG_scan
Scan policy used : Template: DISA STIG WIN 11
Scanner IP : 10.0.0.8
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 15.712 ms
Thorough tests : yes
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 : 80
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/12/18 18:09 UTC
Scan duration : 1126 sec
Scan for malware : no
```

21745 (1) - OS Security Patch Assessment Failed

Synopsis

Errors prevented OS Security Patch Assessment.

Description

OS Security Patch Assessment is not available for this host because either the credentials supplied in the scan policy did not allow Nessus to log into it or some other problem occurred.

Solution

Fix the problem(s) so that OS Security Patch Assessment is possible.

Risk Factor

None

References

XREF	IAVB-0001-B-0501

Plugin Information:

Publication date: 2006/06/23, Modification date: 2021/07/12

Assets

10.1.0.164 (TCP/0) Vulnerability State: Active

```
The following service errors were logged :

  - Plugin      : smb_login.nasl
    Plugin ID   : 10394
    Plugin Name : Microsoft Windows SMB Log In Possible
    Protocol    : SMB
    Message     :
It was not possible to log into the remote host via smb (invalid credentials).
```

64814 (1) - Terminal Services Use SSL/TLS

Synopsis

The remote Terminal Services use SSL/TLS.

Description

The remote Terminal Services is configured to use SSL/TLS.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2013/02/22, Modification date: 2023/07/10

Assets

10.1.0.164 (TCP/3389) Vulnerability State: Active

```
 Subject Name:

Common Name: LogNPacific3286

Issuer Name:

Common Name: LogNPacific3286

Serial Number: 1E 47 E8 36 4B 74 C3 A9 46 E5 2C 0D 58 B7 FF D5

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Dec 15 16:13:33 2025 GMT
Not Valid After: Jun 16 16:13:33 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 AD 24 55 B1 54 7E E8 51 0E 7C F0 D7 12 21 C5 54 52 50 35
            1B 41 38 B5 92 07 AB DF 29 0B BC 09 D4 BB BA 01 A9 F1 9E 96
            E5 2A A3 7E A4 14 E6 6A 4E D9 01 10 D1 95 88 EC F6 AF 5E 29
            03 71 63 9E 71 59 0B 0F F5 9B 99 93 A6 88 9B CE CC EA C4 DD
            E8 CB D1 95 DF 18 45 65 4B 12 17 D3 64 35 11 2A 0A 14 AF E0
            59 43 E9 DD 71 B4 7D D8 C8 99 40 7D C8 70 0F 36 A9 CE 01 35
            97 70 E7 61 AA EF 81 48 B4 15 22 28 FF 53 5A 42 C0 DE EA C6
            27 40 FF 7B 09 BD 76 FA 09 1B 73 A4 AC 66 D7 95 F5 E1 5D 84
            53 E9 5A F7 DD 20 7C B0 96 DF 75 06 04 1E 7B 8C 6D 0B 38 35
            98 DA 4B 5E 54 17 13 DB 6F DC 68 A9 AB F4 F0 E0 A8 40 44 09
            50 DE F9 59 28 6A B5 94 33 B1 DF FD 8A E4 04 E5 D0 18 C6 59
            8E 95 81 84 B0 BE 36 1B 27 9D AD 08 5D DC 08 93 0F 3D DD 6F
            3D 9D 5F 1F C2 69 8B D1 D5 8E 6D D9 80 6A 48 4C A1
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 00 DA B8 5E E3 9C D9 6B C2 5A F0 6D 10 C0 14 4D 0E E8 4F
           FA FA 24 E2 23 E1 CE 26 71 4E 39 0F 49 77 0C B1 B7 FE 8C D1
           C7 2A E1 15 C6 FD 40 59 82 A2 68 C0 E2 9E CC 18 6C 9C 19 2A
           9D 05 7F 85 00 38 84 91 FD A5 58 84 34 F6 72 73 16 DB 9C AC
           B3 B5 DA 76 2B DF 10 F1 A7 33 19 EF 98 5E 49 C0 15 F6 D5 5C
           80 2B 8E 36 EB E2 35 0C 1E 9B 8D 69 24 3E 4D 17 D3 2A C5 AD
           EB 9C D3 15 CA 63 7D 79 36 6C BE 51 69 A0 48 E0 71 51 AE 30
           20 C9 70 87 F3 A1 8E 55 EE 41 21 BE 7C AF B1 EF D5 12 A3 DB
           20 2B 8F C3 10 E8 23 BE 7D 47 96 E3 A8 C8 70 BE FF E7 AD A4
           C8 F2 DE D1 E2 56 [...]
```

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/man1.0.2/man1/ciphers.html

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

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2024/09/11

Assets

10.1.0.164 (TCP/3389) Vulnerability State: Active

```
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_256_GCM_SHA384        0x13, 0x02       -             -        AES-GCM(256)
 SHA384


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

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     --------------------
 ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DHE           RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DHE           RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDHE         RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDHE         RSA      AES-GCM(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDHE         RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDHE         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
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDHE         RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDHE         RSA      AES-CBC(256)
 SHA384
```

RSA-AES128-SHA256	0x00, 0x3C	RSA	[...]

10335 (1) - 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:

Publication date: 2009/02/04, Modification date: 2025/07/14

Assets

10.1.0.164 (TCP/0) Vulnerability State: Active


```
 {"listening":
[{"port":139,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"smb","plugin_output":nu
{"port":135,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"epmap","plugin_output":n
{"port":445,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":null,"plugin_output":null
{"port":3389,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"msrdp","plugin_output":
{"TCP":{"discrete":
[7,9,11,13,15,27,29,31,33,35,333,702,721,723,744,767,808,810,860,871,873,898,927,950,953,975,1005,1008,1010,10
 [...]
```

54615 (1) - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2025/03/12

Assets

10.1.0.164 (TCP/0) Vulnerability State: Active

```
Remote device type : unknown
Confidence level : 56
```

156899 (1) - 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:

Publication date: 2022/01/20, Modification date: 2024/02/12

Assets

10.1.0.164 (TCP/3389) Vulnerability State: Active

```
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      DHE          RSA      AES-GCM(128)
SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F      DHE          RSA      AES-GCM(256)
SHA384
    RSA-AES128-SHA256             0x00, 0x9C      RSA          RSA      AES-GCM(128)
SHA256
    RSA-AES256-SHA384             0x00, 0x9D      RSA          RSA      AES-GCM(256)
SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13      ECDHE        RSA      AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14      ECDHE        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
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27      ECDHE        RSA      AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28      ECDHE        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

The fields above are :

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

104410 (1) - Target Credential Status by Authentication Protocol - Failure for Provided Credentials

Synopsis

Nessus was unable to log into the detected authentication protocol, using the provided credentials, in order to perform credentialed checks.

Description

Nessus failed 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 failure in protocol negotiation or communication that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may have been invalid. A protocol failure may indicate a compatibility issue with the protocol configuration. A protocol failure due to an environmental issue such as resource or congestion issues may also prevent valid credentials from being identified. 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

Address the reported problem(s) so that credentialed checks can be executed.

Risk Factor

None

References

XREF	IAVB-0001-B-0503

Plugin Information:

Publication date: 2017/11/06, Modification date: 2020/10/19

Assets

10.1.0.164 (TCP/139) Vulnerability State: Active

```
Nessus was unable to log into the following host for which
credentials have been provided :

  Protocol        : SMB
  Port            : 139
  Failure details :

  - User : SantiagoX86

    - Plugin      : smb_login.nasl
      Plugin ID   : 10394
      Plugin Name : Microsoft Windows SMB Log In Possible
      Message     : netbios_session_request() failed.


    - Plugin      : smb_login.nasl
      Plugin ID   : 10394
      Plugin Name : Microsoft Windows SMB Log In Possible
      Message     :
Failed to authenticate using the supplied credentials.
```

106716 (1) - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2018/02/09, Modification date: 2020/03/11

Assets

10.1.0.164 (TCP/139) Vulnerability State: Active

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

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:

Publication date: 1999/11/27, Modification date: 2023/12/04

Assets

10.1.0.164 (UDP/0) Vulnerability State: Active

```
For your information, here is the traceroute from 10.0.0.8 to 10.1.0.164 :
10.0.0.8
10.1.0.164

Hop Count: 1
```

11936 (1) - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2025/06/03

Assets

10.1.0.164 (TCP/0) Vulnerability State: Active

```
Remote operating system : Microsoft Windows Server 2025
Confidence level : 56
Method : MLSinFP

Not all fingerprints could give a match. If you think that these
signatures would help us improve OS fingerprinting, please submit
them by visiting https://www.tenable.com/research/submitsignatures.

ICMP:!::0:1:0:128:1:128:1:0:::0::1:X:X:X:X:X:X:X:X:X:1:1:128:65535:MNWST:8:1:1
SinFP:!:
   P1:B11113:F0x12:W8192:O0204ffff:M1410:
   P2:B11113:F0x12:W8192:O0204ffff010303080402080affffffff44454144:M1410:
   P3:B00000:F0x00:W0:O0:M0
   P4:191601_7_p=139R
SSLcert:!:i/CN:LogNPacific3286s/CN:LogNPacific3286
5b338aae80435664bd27c053115a00e3c71fc72a



The remote host is running Microsoft Windows Server 2025
```

10736 (8) - DCE Services Enumeration

Synopsis

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

Description

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

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2001/08/26, Modification date: 2021/10/04

Assets

10.1.0.164 (TCP/49665) Vulnerability State: Active

```
The following DCERPC services are available on TCP port 49665 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49665
IP : 10.1.0.164
```

10.1.0.164 (TCP/49667) Vulnerability State: Active

```
The following DCERPC services are available on TCP port 49667 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Windows Event Log
Type : Remote RPC service
TCP Port : 49667
IP : 10.1.0.164

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49667
IP : 10.1.0.164

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49667
IP : 10.1.0.164
```

10.1.0.164 (TCP/139) Vulnerability State: Active

```
The following DCERPC services are available remotely :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f1343fe-50a9-4927-a778-0c5859517bac, version 1.0
Description : Unknown RPC service
Annotation : DfsDs service
```

```
Type : Remote RPC service
Named pipe : \PIPE\wkssvc
Netbios name : \\LogNPacific3286

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\LogNPacific3286

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\LogNPacific3286

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 33d84484-3626-47ee-8c6f-e7e98b113be1, version 2.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\LogNPacific3286

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\LogNPacific3286

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\LogNPacific3286

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\LogNPacific3286

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 29770a8f-829b-4158-90a2-78cd488501f7, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\LogNPacific3286

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 29770a8f-829b-4158-90a2-78cd488501f7, [...]
```

10.1.0.164 (TCP/49666) Vulnerability State: Active

```
The following DCERPC services are available on TCP port 49666 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49666
IP : 10.1.0.164

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3a9ef155-691d-4449-8d05-09ad57031823, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49666
```

```
IP : 10.1.0.164

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49666
IP : 10.1.0.164

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 29770a8f-829b-4158-90a2-78cd488501f7, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49666
IP : 10.1.0.164

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49666
IP : 10.1.0.164

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager provider server endpoint
Type : Remote RPC service
TCP Port : 49666
IP : 10.1.0.164

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1.0
Description : Unknown RPC service
Annotation : Proxy Manager client server endpoint
Type : Remote RPC service
TCP Port : 49666
IP : 10.1.0.164

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1.0
Description : Unknown RPC service
Annotation : Adh APIs
Type : Remote RPC service
TCP Port : 49666
IP : 10.1.0.164

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv [...]
```

10.1.0.164 (TCP/49671) Vulnerability State: Active

```
The following DCERPC services are available on TCP port 49671 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49671
IP : 10.1.0.164
```

10.1.0.164 (TCP/49668) Vulnerability State: Active

```
The following DCERPC services are available on TCP port 49668 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
```

```
Type : Remote RPC service
TCP Port : 49668
IP : 10.1.0.164

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49668
IP : 10.1.0.164

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49668
IP : 10.1.0.164

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49668
IP : 10.1.0.164

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 76f03f96-cdfd-44fc-a22c-64950a001209, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49668
IP : 10.1.0.164
```

10.1.0.164 (TCP/135) Vulnerability State: Active

```
The following DCERPC services are available locally :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : samss lpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : SidKey Local End Point

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : protected_storage

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : lsasspirpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : lsapolicylookup

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
```

```
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : LSA_EAS_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : LSA_IDPEXT_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Local RPC service
Named pipe : lsacap

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc [...]
```

10.1.0.164 (TCP/49664) Vulnerability State: Active

```
The following DCERPC services are available on TCP port 49664 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49664
IP : 10.1.0.164

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49664
IP : 10.1.0.164

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
TCP Port : 49664
IP : 10.1.0.164

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1.0
Description : Unknown RPC service
Annotation : Ngc Pop Key Service
Type : Remote RPC service
TCP Port : 49664
IP : 10.1.0.164
```

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:

Publication date: 2011/12/01, Modification date: 2025/06/16

Assets

10.1.0.164 (TCP/3389) Vulnerability State: Active

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

10940 (1) - Remote Desktop Protocol Service Detection

Synopsis

The remote host has an remote desktop protocol service enabled.

Description

The Remote Desktop Protocol allows a user to remotely obtain a graphical login (and therefore act as a local user on the remote host).
If an attacker gains a valid login and password, this service could be used to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.
Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.

Solution

Disable the service if you do not use it, and do not allow this service to run across the Internet.

Risk Factor

None

Plugin Information:

Publication date: 2002/04/20, Modification date: 2023/08/21

Assets

10.1.0.164 (TCP/3389) Vulnerability State: Active

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:

Publication date: 2010/04/21, Modification date: 2025/09/29

Assets

10.1.0.164 (TCP/0) Vulnerability State: Active

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

  cpe:/o:microsoft:windows -> Microsoft Windows
```

277650 (1) - Remote Services Not Using Post-Quantum Ciphers

Synopsis

Reports remote services that do not offer post-quantum ciphers.

Description

This plugin reports network services that do not offer post-quantum ciphers. Tenable makes no attempt to determine whether the remote service would be vulnerable to a post-quantum attack.
However, cryptography that depends on the classic difficulty of solving the discrete logarithm problem or on the classic difficulty of large prime factorization is broken by Shor's algorithm. Examples of this are RSA asymmetric encryption and Diffie-Hellman key exchange.

See Also

http://www.nessus.org/u?7a390f87

http://www.nessus.org/u?ad7d6b3b

http://www.nessus.org/u?1c0c61e0

http://www.nessus.org/u?5eec4b28

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2025/12/08, Modification date: 2025/12/08

Assets

10.1.0.164 (TCP/3389) Vulnerability State: Active

```
The target TLS server offers no post-quantum ciphers.
```

277654 (1) - TLS Supported Groups

Synopsis

The remote service negotiates TLS supported curve groups.

Description

This plugin detects which TLS supported groups entries are supported by the remote service.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2025/12/08, Modification date: 2025/12/10

Assets

10.1.0.164 (TCP/3389) Vulnerability State: Active

```
These are the TLS supported groups offered by the remote server :


TLS supported groups :

Name                Code
--------------------------
x25519              0x001d
secp384r1           0x0018
secp256r1           0x0017
```

209654 (1) - 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:

Publication date: 2025/02/26, Modification date: 2025/03/03

Assets

10.1.0.164 (TCP/0) Vulnerability State: Active

```
Following OS Fingerprints were found

Remote operating system : Microsoft Windows Server 2025
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Windows
Confidence level : 50
Method : Misc
Type : general-purpose
Fingerprint : unknown

Following fingerprints could not be used to determine OS :
 ICMP:!::0:1:0:128:1:128:1:0:::0::1:X:X:X:X:X:X:X:X:X:1:1:128:65535:MNWST:8:1:1
SinFP:!:
   P1:B11113:F0x12:W8192:O0204ffff:M1410:
   P2:B11113:F0x12:W8192:O0204ffff010303080402080affffffff44454144:M1410:
   P3:B00000:F0x00:W0:O0:M0
   P4:191601_7_p=139R
SSLcert:!:i/CN:LogNPacific3286s/CN:LogNPacific3286
5b338aae80435664bd27c053115a00e3c71fc72a
```

11011 (1) - Microsoft Windows SMB Service Detection

Synopsis

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

Description

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

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2021/02/11

Assets

10.1.0.164 (TCP/139) Vulnerability State: Active

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

Assets Summary (Executive)

10.1.0.164

Summary

Critical	High	Medium	Low	Info	Total
0	0	2	1	25	28

Details

Severity	Plugin Id	Name
Medium	57582	SSL Self-Signed Certificate
Medium	51192	SSL Certificate Cannot Be Trusted
Low	10114	ICMP Timestamp Request Remote Date Disclosure
Info	136318	TLS Version 1.2 Protocol Detection
Info	138330	TLS Version 1.3 Protocol Detection
Info	10863	SSL Certificate Information
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	19506	Nessus Scan Information
Info	21745	OS Security Patch Assessment Failed
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	25220	TCP/IP Timestamps Supported
Info	64814	Terminal Services Use SSL/TLS
Info	21643	SSL Cipher Suites Supported
Info	10335	Nessus TCP scanner
Info	54615	Device Type
Info	10287	Traceroute Information
Info	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
Info	104410	Target Credential Status by Authentication Protocol - Failure for Provided Credentials
Info	156899	SSL/TLS Recommended Cipher Suites
Info	11936	OS Identification
Info	10736	DCE Services Enumeration
Info	10940	Remote Desktop Protocol Service Detection
Info	56984	SSL / TLS Versions Supported
Info	277650	Remote Services Not Using Post-Quantum Ciphers
Info	45590	Common Platform Enumeration (CPE)
Info	209654	OS Fingerprints Detected

Info	277654	TLS Supported Groups
Info	11011	Microsoft Windows SMB Service Detection