OT Seksi Plastic Injection P3

Report generated by Nessus™ Tue, 27 Feb 2024 08:48:06 WIB

TABLE OF CONTENTS

Vulnerabilities by Host

- 172.26.12.2..... 4

Vulnerabilities by Host

172.26.12.2

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	10

Scan Information

Start time: Tue Feb 27 08:43:00 2024
End time: Tue Feb 27 08:48:06 2024

Host Information

IP: 172.26.12.2

Vulnerabilities

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/02/21

Plugin Output

tcp/22/ssh

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

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

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

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

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/02/21

Plugin Output

tcp/1720

```
Port 1720/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

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

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.

- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2023/07/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.6.3
Nessus build : 20009
Plugin feed version : 202402262301
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : es7-x86-64
Scan type : Normal
Scan name : OT Seksi Plastic Injection P3
Scan policy used : Basic Network Scan
Scanner IP : 10.9.10.122
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 24.838 ms
Thorough tests : no
Experimental tests : 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 launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
```

```
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/2/27 8:43 WIB
Scan duration : 274 sec
Scan for malware : no
```

50350 - 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

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.

SSH:!:SSH-2.0--
SinFP:!:
   P1:B11013:F0x12:W8192:O0204ffff:M1460:
   P2:B11013:F0x12:W8192:O0204ffff:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:190703_7_p=22R
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

The server supports the following options for kex_algorithms :

  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha256
  diffie-hellman-group15-sha512
  diffie-hellman-group16-sha512

The server supports the following options for server_host_key_algorithms :

  rsa-sha2-256
  rsa-sha2-512

The server supports the following options for encryption_algorithms_client_to_server :

  aes128-ctr
  aes256-ctr

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-ctr
  aes256-ctr

The server supports the following options for mac_algorithms_client_to_server :

  hmac-sha2-256

The server supports the following options for mac_algorithms_server_to_client :

  hmac-sha2-256

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

```
  none
  zlib

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib
```

149334 - 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

tcp/22/ssh

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/22/ssh

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

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

tcp/22/ssh

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

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.9.10.122 to 172.26.12.2 :
10.9.10.122
10.9.10.1
192.200.5.1
10.9.10.1
10.4.254.9
10.13.0.171
?
172.26.0.1
172.26.12.2

Hop Count: 9
```