scan2

Report generated by Nessus™ Mon, 16 Oct 2023 14:55:13 SA Pacific Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.20.177

0	0	0	1	4
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Mon Oct 16 14:50:04 2023
End time: Mon Oct 16 14:55:13 2023

Host Information

IP: 192.168.20.177
MAC Address: 76:AC:EA:2C:43:08

Vulnerabilities

11197 - Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)

Synopsis

The remote host appears to leak memory in network packets.

Description

The remote host uses a network device driver that pads ethernet frames with data which vary from one packet to another, likely taken from kernel memory, system memory allocated to the device driver, or a hardware buffer on its network interface card.

Known as 'Etherleak', this information disclosure vulnerability may allow an attacker to collect sensitive information from the affected host provided he is on the same physical subnet as that host.

See Also

http://www.nessus.org/u?719c90b4

Solution

Contact the network device driver's vendor for a fix.

Risk Factor

Low

VPR Score

4.2

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID	6535
CVE	CVE-2003-0001

Plugin Information

Published: 2003/01/14, Modified: 2019/03/06

Plugin Output

icmp/0

```
Padding observed in one frame :

  0x00:  77 4F CA 7D 67 E6 00 49 E7 40 C2 D5 2F 3A A0 01    wO.}g..I.@../:..
  0x10:  BB C7 C5 04 D8                                     .....

Padding observed in another frame :

  0x00:  B5 00 01 02 00 00 00 E0 00 00 FB 12 D0 FA 2C 73    ..............,s
  0x10:  6D 0A 48 4F 53                                     m.HOS
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 76:AC:EA:2C:43:08
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

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

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

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

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2023/04/27

Plugin Output

icmp/0

```
The difference between the local and remote clocks is 15 seconds.
```

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 : 10.5.5
Nessus build : 20002
Plugin feed version : 202310161413
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : scan2
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.20.44
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 196.391 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 : 2023/10/16 14:50 SA Pacific Standard Time
Scan duration : 302 sec
Scan for malware : no
```

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: 2023/06/26

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.20.44 to 192.168.20.177 :
192.168.20.44
192.168.20.177

Hop Count: 1
```