test

Wed, 24 Jan 2024 13:05:39 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

18.192.172.30

0	0	0	0	3
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

DNS Name:	ec2-18-192-172-30.eu-central-1.compute.amazonaws.com
IP:	18.192.172.30

Vulnerabilities

12053 - Host Fully Qualified Domain Name (FQDN) Resolution -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
18.192.172.30 resolves as ec2-18-192-172-30.eu-central-1.compute.amazonaws.com.
```

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- Whether the display of superseded patches is enabled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 : 10.6.4
Nessus build : 20005
Plugin feed version : 202401240348
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : test
Scan policy used : test
Scanner IP : 10.15.192.220
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 33.033 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Display superseded patches : yes (supersedence plugin launched)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 : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/1/24 11:59 India Standard Time
Scan duration : 3966 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: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.15.192.220 to 18.192.172.30 :
10.15.192.220

ttl was greater than 50 - Completing Traceroute.

10.15.192.10
115.242.182.201
?
172.16.92.145
103.198.140.174
49.45.4.65
52.95.218.74
?

Hop Count: 9

An error was detected along the way.
```