



Team ID 591486

Report generated by Nessus™

Tue, 24 Oct 2023 19:02:02 India Standard Time

Abirami .r
Niraianbu .p
Kamal nath. r
Tharunya bala s

TABLE OF CONTENTS

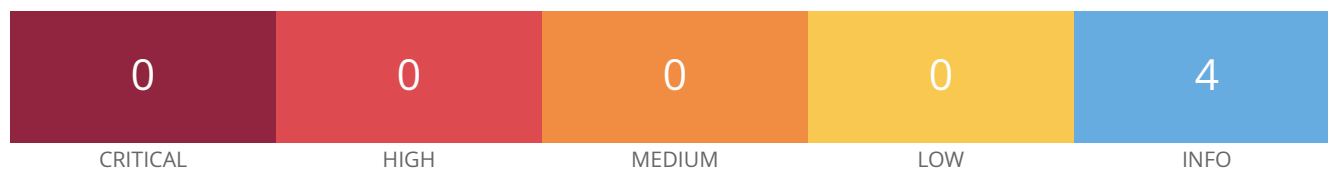
Vulnerabilities by Host

• 46.17.172.80.....	4
---------------------	---

Nessus Essentials

Vulnerabilities by Host

46.17.172.80



Vulnerabilities

Total: 4

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information

* indicates the v3.0 score was not available; the v2.0 score is shown



Team ID 591486

Report generated by Nessus™

Tue, 24 Oct 2023 19:02:02 India Standard Time

Abirami .r
Niraianbu .p
Kamal nath. r
Tharunya bala s

TABLE OF CONTENTS

Vulnerabilities by Host

- 46.17.172.80.....4

Nessus Essentials

Vulnerabilities by Host

46.17.172.80



Scan Information

Start time: Tue Oct 24 18:47:22 2023
End time: Tue Oct 24 19:02:02 2023

Host Information

IP: 46.17.172.80
OS: Linux Kernel 2.6

Vulnerabilities

43111 - 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_\(OTG-CONFIG-006\)](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: 2022/04/11

Plugin Output

tcp/80/www

Based on tests of each method :

- HTTP methods BASELINE-CONTROL CHECKIN CHECKOUT CONNECT COPY
DELETE GET HEAD LABEL LOCK MERGE MKACTION MKCOL MKWORKSPACE
MOVE OPTIONS PATCH POST PROPFIND PROPPATCH PUT REPORT SEARCH
TRACE UNCHECKOUT UNLOCK UPDATE VERSION-CONTROL are allowed on :

/

10107 - 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

tcp/80/www

```
The remote web server type is :  
LiteSpeed
```

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: 2023/09/25

Plugin Output

tcp/21/ftp

```
Port 21/tcp was found to be open
```

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: 2023/09/25

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

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: 2023/09/25

Plugin Output

tcp/443

```
Port 443/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: 2023/09/25

Plugin Output

tcp/3306/mysql

```
Port 3306/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 : 10.6.0
Nessus build : 20103
Plugin feed version : 202310180342
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : love
```

```
Scan policy used : Web Application Tests
Scanner IP : 192.168.43.106
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 246.636 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 : enabled
Web application tests : enabled
Web app tests - Test mode : single
Web app tests - Try all HTTP methods : no
Web app tests - Maximum run time : 5 minutes.
Web app tests - Stop at first flaw : CGI
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 : 2023/10/24 18:47 India Standard Time
Scan duration : 869 sec
Scan for malware : no
```