Report generated by Tenable Nessus™

web_app_wks2_physio

Sat, 08 Mar 2025 13:37:25 FLE Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.100.100

0	0	0	0	12
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Sat Mar 8 13:27:49 2025
End time:	Sat Mar 8 13:37:25 2025

Host Information

IP:	192.168.100.100
MAC Address:	00:0C:29:CF:4C:24
OS:	Microsoft Windows 10 Enterprise, Microsoft Windows Server 2019 LTSC, Microsoft Windows Server 2019

Vulnerabilities

49704 - External URLs -

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

Plugin Output

tcp/3001/www

```
  4 external URLs were gathered on this web server :
  URL... - Seen on...

  https://fonts.googleapis.com - /
  https://fonts.googleapis.com/css2?family=Roboto:wght@300;400;500;700&display=swap - /
  https://fonts.googleapis.com/icon?family=Material+Icons - /
  https://fonts.gstatic.com - /
```

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)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/3001/www

```
  Based on tests of each method :

  - HTTP methods ACL CHECKOUT COPY DELETE GET HEAD LOCK MERGE
  MKACTIVITY MKCOL MOVE NOTIFY OPTIONS PATCH POST PROPFIND
  PROPPATCH PUT REPORT SEARCH SUBSCRIBE TRACE UNLOCK UNSUBSCRIBE
  are allowed on :

  /
  /static
  /static/css
```

24260 - HyperText Transfer Protocol (HTTP) Information -

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/3001/www

```

  Response Code : HTTP/1.1 200 OK

  Protocol version : HTTP/1.1
  HTTP/2 TLS Support: No
  HTTP/2 Cleartext Support: No
  SSL : no
  Keep-Alive : yes
  Options allowed : (Not implemented)
  Headers :

  X-Powered-By: Express
  Access-Control-Allow-Origin: *
  Accept-Ranges: bytes
  Cache-Control: public, max-age=0
  Last-Modified: Sat, 01 Mar 2025 20:13:22 GMT
  ETag: W/"3ca-19553578f83"
  Content-Type: text/html; charset=UTF-8
  Content-Length: 970
  Date: Sat, 08 Mar 2025 11:30:30 GMT
  Connection: keep-alive
  Keep-Alive: timeout=5

  Response Body :

  <!doctype html><html lang="en"><head><meta charset="utf-8"/><link rel="icon" href="/favicon.ico"/><meta name="viewport"
  content="width=device-width,initial-scale=1"/><meta name="theme-color" content="#000000"/><meta name="description" content="Web site
  created using create-react-app"/><link rel="apple-touch-icon" href="/logo192.png"/><link rel="manifest" href="/manifest.json"/><link
  rel="preconnect" href="https://fonts.googleapis.com"/><link rel="preconnect" href="https://fonts.gstatic.com" crossorigin/><link
  rel="stylesheet" href="https://fonts.googleapis.com/css2?family=Roboto:wght@300;400;500;700&display=swap"/><link rel="stylesheet"
  href="https://fonts.googleapis.com/icon?family=Material+Icons"/><title>Physio</title><script defer="defer"
  src="/static/js/main.37168ee9.js"></script><link href="/static/css/main.3784df71.css" rel="stylesheet"></head><body><noscript>You
  need to enable JavaScript to run this app.</noscript><div id="root"></div></body></html>
```

50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header -

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://www.nessus.org/u?55aa8f57
http://www.nessus.org/u?07cc2a06
https://content-security-policy.com/
https://www.w3.org/TR/CSP2/

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/3001/www

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a permissive policy:

- http://WKS2:3001/
```

50345 - Missing or Permissive X-Frame-Options HTTP Response Header -

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

https://en.wikipedia.org/wiki/Clickjacking
http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/3001/www

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

- http://WKS2:3001/
```

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: 2025/02/12

Plugin Output

tcp/135/epmap

```
  Port 135/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: 2025/02/12

Plugin Output

tcp/139/smb

```
  Port 139/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: 2025/02/12

Plugin Output

tcp/445/cifs

```
Port 445/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: 2025/02/12

Plugin Output

tcp/3001/www

```
Port 3001/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: 2024/12/31

Plugin Output

tcp/0

```
  Information about this scan :

  Nessus version : 10.8.3
  Nessus build : 20010
  Plugin feed version : 202503070251
  Scanner edition used : Nessus Home
  Scanner OS : WINDOWS
  Scanner distribution : win-x86-64
  Scan type : Normal
  Scan name : web_app_wks2_physio
  Scan policy used : Web Application Tests
  Scanner IP : 192.168.100.11
  Port scanner(s) : nessus_syn_scanner
  Port range : default
  Ping RTT : 0.958 ms
  Thorough tests : no
  Experimental tests : no
  Scan for Unpatched Vulnerabilities : no
  Plugin debugging enabled : no
  Paranoia level : 1
  Report verbosity : 1
  Safe checks : yes
  Optimize the test : no
  Credentialed checks : no
  Patch management checks : None
  Display superseded patches : yes (supersedence plugin did not launch)
  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 : 2025/3/8 13:28 FLE Standard Time (UTC +02:00)
  Scan duration : 565 sec
  Scan for malware : no
```

91815 - Web Application Sitemap -

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

tcp/3001/www

```
  The following sitemap was created from crawling linkable content on the target host :

  - http://WKS2:3001/
  - http://WKS2:3001/favicon.ico
  - http://WKS2:3001/logo192.png
  - http://WKS2:3001/manifest.json
  - http://WKS2:3001/static/css/main.3784df71.css

Attached is a copy of the sitemap file.
```

10302 - Web Server robots.txt Information Disclosure -

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/3001/www

```
Contents of robots.txt :

# https://www.robotstxt.org/robotstxt.html
User-agent: *
Disallow:
```