



TAP_Business_Website

Report generated by Nessus™

Sat, 06 Apr 2024 11:23:01 PDT

TABLE OF CONTENTS

Vulnerabilities by Host

• theaccountabilitypartners.net.....	4
--------------------------------------	---

Nessus Essentials

Vulnerabilities by Host

theaccountabilitypartners.net



Scan Information

Start time: Sat Apr 6 11:06:52 2024
End time: Sat Apr 6 11:23:01 2024

Host Information

DNS Name: aacb0a264e514dd48.awsglobalaccelerator.com
IP: 99.83.190.102

Vulnerabilities

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

<https://tools.ietf.org/html/rfc6797>

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2021/05/19

Plugin Output

tcp/443/www

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

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/443/www

Based on tests of each method :

- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD INDEX LABEL LOCK MERGE MKACTION MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE UNCHECKOUT UNLOCK UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

/

- Invalid/unknown HTTP methods are allowed on :

/

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/443/www

```
Response Code : HTTP/1.1 301 Moved Permanently

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

    Date: Sat, 06 Apr 2024 18:15:11 GMT
    Content-Type: text/html
    Content-Length: 166
    Connection: keep-alive
    Location: https://www.theaccountabilitypartners.net/

Response Body :

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>openresty</center>
</body>
</html>
```


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: 2024/03/19

Plugin Output

tcp/80

```
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: 2024/03/19

Plugin Output

tcp/443/www

```
Port 443/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: 2024/03/13

Plugin Output

tcp/0

Information about this scan :

```
Nessus version : 10.7.2
Nessus build : 20029
Plugin feed version : 202404061459
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1804-aarch64
Scan type : Normal
Scan name : TAP_Business_Website
```

```
Scan policy used : Web Application Tests
Scanner IP : 172.16.248.128
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 47.356 ms
Thorough tests : no
Experimental tests : 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 : 2024/4/6 11:07 PDT
Scan duration : 959 sec
Scan for malware : no
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/443/www

```
CGI scanning will be disabled for this host because the host responds  
to requests for non-existent URLs with HTTP code 301  
rather than 404. The requested URL was :
```

```
https://theaccountabilitypartners.net/boDHjX4xacmG.html
```