VA Report (Scan: Adhoc-172.26.193.156)

Generated on May 12, 2023 at 6:15 AM UTC

Imported on May 12, 2023 at 6:14 AM UTC (Scan Result ID #37222)

Gihan Thirimanne [gihan_08352]
DIALOG AXIATA PLC

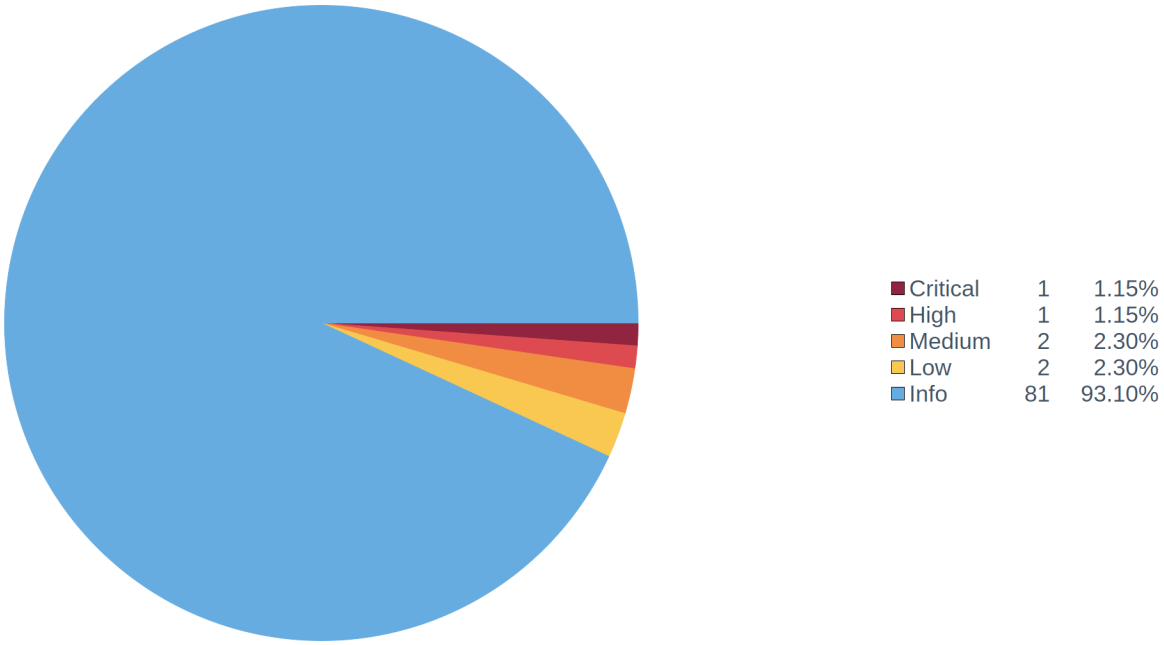
Table of Contents

Executive Summary

This chapter provides as overview of the results of Nessus scans. Each component provides a different view of the vulnerabilities detected by Nessus.

The Severity Summary pie chart displays a breakdown of the current vulnerabilities found in the network based on their severity. This chart is useful for understanding the overall vulnerability status of the network based on severity and can assist teams in determining where their mitigation or compliance efforts will be most impactful.

Severity Summary



The Host Summary table displays the top ten hosts by vulnerability score. This table displays the IP address, DNS name, and a vulnerability bar for each host. This table can help security teams determine which hosts are the most vulnerable within the network.

Host Summary

IP Address	DNS Name	Score	Low	Med.	High	Crit.	Total	Vulns
172.26.193.156		58	2	2	1	1	87	81

Vulnerabilities by Host

This chapter contains an iterator that lists scanned IP addresses and detailed information about vulnerabilities detected on each. The DNS name, NetBIOS name, MAC address, repository, total vulnerability count, and last scan date are included for each IP address. The Results Summary table displays the number of vulnerabilities found on that host by severity. The Results Details table lists detailed information for each vulnerability detected, including the plugin ID, plugin name, plugin family, severity, protocol, port used, exploitability, and CPE. The plugin text, including the synopsis, description, solution, risk factor, and plugin output, is also included in the table. Lastly, the first detected and last observed dates are noted for each vulnerability.

172.26.193.156

IP Address: 172.26.193.156
MAC Address: 00:50:56:87:31:4d
Score: 58
Repository: Individual Scan (id: Individual Scan)
Total: 87

Results Summary

Severity	Count
Critical	1
High	1
Medium	2
Low	2
Info	81

Severity Summary

IP Address	NetBIOS Name	DNS Name	Score	Med.	High	Crit.	Total	Vulns
172.26.193.156			56	2	1	1	4	1 1 2

Vulnerability List

Plugin Name	Severity	IP Address
HTTP TRACE / TRACK Methods Allowed	Medium	172.26.193.156
Web Application Potentially Vulnerable to Clickjacking	Medium	172.26.193.156
PHP 8.0.x < 8.0.27	Critical	172.26.193.156
PHP 8.0.x < 8.0.28	High	172.26.193.156

Results Details

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port	Exploit?
11213	HTTP TRACE / TRACK Methods Allowed	Web Servers	Medium	172.26.193.156	TCP	80	No
Plugin Output: **Plugin Output**:							

To disable these methods, add the following lines for each virtual
host in your configuration file :

RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

```
------------------------------ snip ------------------------------
TRACE /Nessus2145226129.html HTTP/1.1
Connection: Close
Host: 172.26.193.156
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

and received the following response from the remote server :

```
------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Fri, 12 May 2023 05:59:23 GMT
Server: Apache/2.4.37 (Red Hat Enterprise Linux)
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus2145226129.html HTTP/1.1
Connection: Keep-Alive
Host: 172.26.193.156
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

Synopsis: Debugging functions are enabled on the remote web server.

Description: The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Solution: Disable these HTTP methods. Refer to the plugin output for more information.

See Also: https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
https://download.oracle.com/sunalerts/1000718.1.html

STIG Severity:

CVSS V3 Base Score: 5.3

CVSS V3 Temporal Score: 4.6

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O/RC:C

CPE:

CVE: CVE-2003-1567,CVE-2004-2320,CVE-2010-0386

BID: 9506,9561,11604,33374,37995

Cross References: CERT #288308,CERT #867593,CWE #16,CWE #200

First Discovered: Apr 11, 2023 03:53:39 UTC

Last Observed: May 12, 2023 06:15:06 UTC

Vuln Publication Date: Jan 20, 2003 12:00:00 UTC

Patch Publication Date: N/A

Plugin Publication Date: Jan 23, 2003 12:00:00 UTC

Plugin Modification Date: Jun 12, 2020 12:00:00 UTC

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port	Exploit?
85582	Web Application Potentially Vulnerable to Clickjacking	Web Servers	Medium	172.26.193.156	TCP	8000	No

Plugin Output:

Plugin Output:
The following pages do not use a clickjacking mitigation response header and contain a clickable event :

- http://172.26.193.156:8000/

Synopsis: The remote web server may fail to mitigate a class of web application vulnerabilities.

Description: The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

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

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

Solution: Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

See Also: http://www.nessus.org/u?399b1f56
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet
https://en.wikipedia.org/wiki/Clickjacking

STIG Severity:

CVSS V3 Base Score:

CVSS V3 Temporal Score:

CVSS V3 Vector:

CPE:

CVE:

BID:

Cross References: CWE #693

First Discovered: Apr 11, 2023 03:53:39 UTC

Last Observed: May 12, 2023 06:15:06 UTC

Vuln Publication Date: N/A

Patch Publication Date: N/A

Plugin Publication Date: Aug 22, 2015 12:00:00 UTC

Plugin Modification Date: May 16, 2017 12:00:00 UTC

Exploit Ease:

Exploit Frameworks:

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port	Exploit?
169630	PHP 8.0.x < 8.0.27	CGI abuses	Critical	172.26.193.156	TCP	8000	No

Plugin Output:

Plugin Output:
URL : http://172.26.193.156:8000/ (8.0.26 under X-Powered-By: PHP/8.0.26)
Installed version : 8.0.26
Fixed version : 8.0.27

Synopsis: The version PHP running on the remote web server is affected by a vulnerability.

Description: The version of PHP installed on the remote host is prior to 8.0.27. It is, therefore, affected by a vulnerability as referenced in the Version 8.0.27 advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution: Upgrade to PHP version 8.0.27 or later.

See Also: http://bugs.php.net/81740
http://php.net/ChangeLog-8.php#8.0.27

STIG Severity: I

CVSS V3 Base Score: 9.1

CVSS V3 Temporal Score: 7.9

CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C

CPE: cpe:/a:php:php

CVE: CVE-2022-31631

BID:

Cross References: IAVA #2023-A-0016-S

First Discovered: Apr 11, 2023 03:53:39 UTC

Last Observed: May 12, 2023 06:15:06 UTC

Vuln Publication Date: Jan 5, 2023 12:00:00 UTC

Patch Publication Date: Jan 5, 2023 12:00:00 UTC

Plugin Publication Date: Jan 6, 2023 12:00:00 UTC

Plugin Modification Date: Feb 16, 2023 12:00:00 UTC

Exploit Ease: No known exploits are available

Exploit Frameworks:

Plugin	Plugin Name	Family	Severity	IP Address	Protocol	Port	Exploit?
171436	PHP 8.0.x < 8.0.28	CGI abuses	High	172.26.193.156	TCP	8000	No

Plugin Output:

Plugin Output:
URL : http://172.26.193.156:8000/ (8.0.26 under X-Powered-By: PHP/8.0.26)
Installed version : 8.0.26
Fixed version : 8.0.28

Synopsis: The version PHP running on the remote web server is affected by a vulnerability.

Description: The version of PHP installed on the remote host is prior to 8.0.28. It is, therefore, affected by a vulnerability as referenced in the Version 8.0.28 advisory.

- In PHP 8.0.X before 8.0.28, 8.1.X before 8.1.16 and 8.2.X before 8.2.3, excessive number of parts in HTTP form upload can cause high resource consumption and excessive number of log entries. This can cause denial of service on the affected server by exhausting CPU resources or disk space. (CVE-2023-0662)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.
Solution: Upgrade to PHP version 8.0.28 or later.
See Also: http://php.net/ChangeLog-8.php#8.0.28
STIG Severity: I
CVSS V3 Base Score: 7.5
CVSS V3 Temporal Score: 6.5
CVSS V3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C
CPE: cpe:/a:php:php
CVE: CVE-2023-0662
BID:
Cross References: IAVA #2023-A-0105
First Discovered: Apr 11, 2023 03:53:39 UTC
Last Observed: May 12, 2023 06:15:06 UTC
Vuln Publication Date: Feb 14, 2023 12:00:00 UTC
Patch Publication Date: Feb 14, 2023 12:00:00 UTC
Plugin Publication Date: Feb 14, 2023 12:00:00 UTC
Plugin Modification Date: Mar 21, 2023 12:00:00 UTC
Exploit Ease: No known exploits are available
Exploit Frameworks: