Scan Report

June 28, 2024

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "UTC", which is abbreviated "UTC". The task was "Vuln Scanning". The scan started at Fri Jun 28 04:37:01 2024 UTC and ended at Fri Jun 28 06:34:41 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
44.228.249.3 ec2-44-228-249-3.us-west-2.compute.amazonaws.com	0	2	1	0	0
Total: 1	0	2	1	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 3 results selected by the filtering described above. Before filtering there were 60 results.

2 Results per Host

2.1 44.228.249.3

Host scan start	Fri Jun 28 04:37:24 2024 UTC
Host scan end	Fri Jun 28 06:34:32 2024 UTC

Service (Port)	Threat Level
80/tcp	Medium
general/tcp	Low

2.1.1 Medium 80/tcp

Medium (CVSS: 5.3)

NVT: phpinfo() Output Reporting (HTTP)

Summary
Reporting of files containing the output of the phpinfo() PHP function previously detected via HTTP.

Quality of Detection: 80

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result

```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information:
http://testphp.vulnweb.com/secured/phpinfo.php
Concluded from:
  <title>phpinfo()</title></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/usr/lo
↪cal/etc/php.ini </td></tr>
  <h2>PHP Variables</h2>
```

Impact

Some of the information that can be gathered from this file includes:
The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.

Solution:

Solution type: Workaround
Delete the listed files or restrict access to them.

Affected Software/OS

All systems exposing a file containing the output of the phpinfo() PHP function.
This VT is also reporting if an affected endpoint for the following products have been identified:
- CVE-2008-0149: TUTOS
- CVE-2023-49282, CVE-2023-49283: Microsoft Graph PHP SDK

Vulnerability Insight

Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory.

Vulnerability Detection Method

This script reports files identified by the following separate VT: 'phpinfo() Output Detection (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.108474).
Details: `phpinfo() Output Reporting (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: `2023-12-14T08:20:35Z`

References

```
cve: CVE-2008-0149
cve: CVE-2023-49282
cve: CVE-2023-49283
url: https://www.php.net/manual/en/function.phpinfo.php
```

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Quality of Detection: 80

Vulnerability Detection Result
`The following input fields were identified (URL:input name):`
`http://testphp.vulnweb.com/login.php:pass`
`http://testphp.vulnweb.com/signup.php:upass`

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

References
`url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se`
`↪ssion_Management`
`url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure`
`url: https://cwe.mitre.org/data/definitions/319.html`

[return to 44.228.249.3]

2.1.2 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Quality of Detection: 80

Vulnerability Detection Result
```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 3122536422
Packet 2: 3122537766
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP Timestamps Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

References
`url: https://datatracker.ietf.org/doc/html/rfc1323`

... continues on next page ...

... continued from previous page ...

```
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[return to 44.228.249.3]
