Scan Report

June 2, 2024

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “WorstWesternHotel”. The scan started at Thu May 30 13:51:56 2024 UTC and ended at Thu May 30 14:41:33 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
10.0.2.9 prime.worstwestern.com	0	1	2	0	0
Total: 1	0	1	2	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 52 results.

2 Results per Host

2.1 10.0.2.9

Host scan start	Thu May 30 13:52:32 2024 UTC
Host scan end	Thu May 30 14:41:30 2024 UTC

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

2.1.1 Medium 80/tcp

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.

. . . continues on next page . . .

. . . continued from previous page . . .

Quality of Detection: 80

Vulnerability Detection Result

```
The following URLs requires Basic Authentication (URL:realm name):
http://prime.worstwestern.com/api/1:"Welcome to PrestaShop Webservice, please en
↪ter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/2.1/rest:"Welcome to PrestaShop Webservice, pl
↪ease enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/2.1:"Welcome to PrestaShop Webservice, please
↪enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/2:"Welcome to PrestaShop Webservice, please en
↪ter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/ApplicationService:"Welcome to PrestaShop Webs
↪ervice, please enter the authentication key as the login. No password required
↪."
http://prime.worstwestern.com/api/config/class:"Welcome to PrestaShop Webservice
↪, please enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/config:"Welcome to PrestaShop Webservice, plea
↪se enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/explorer:"Welcome to PrestaShop Webservice, pl
↪ease enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/hassio/app:"Welcome to PrestaShop Webservice,
↪please enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/hassio:"Welcome to PrestaShop Webservice, plea
↪se enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/hassio_ingress:"Welcome to PrestaShop Webservi
↪ce, please enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/json/nfausers:"Welcome to PrestaShop Webservic
↪e, please enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/json:"Welcome to PrestaShop Webservice, please
↪ enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/jsonws:"Welcome to PrestaShop Webservice, plea
↪se enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/ldap/config/ldapTreeNodeChildren:"Welcome to P
↪restaShop Webservice, please enter the authentication key as the login. No pas
↪sword required."
http://prime.worstwestern.com/api/ldap/config:"Welcome to PrestaShop Webservice,
↪ please enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/ldap:"Welcome to PrestaShop Webservice, please
↪ enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/platform:"Welcome to PrestaShop Webservice, pl
↪ease enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/repos/dashboards:"Welcome to PrestaShop Webser
↪vice, please enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/repos:"Welcome to PrestaShop Webservice, pleas
↪e enter the authentication key as the login. No password required."
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
http://prime.worstwestern.com/api/system/v1:"Welcome to PrestaShop Webservice, p
↪lease enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/system:"Welcome to PrestaShop Webservice, plea
↪se enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/userrolelist:"Welcome to PrestaShop Webservice
↪, please enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/v1.0:"Welcome to PrestaShop Webservice, please
↪ enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/v1/authentication/connection-token:"Welcome to
↪ PrestaShop Webservice, please enter the authentication key as the login. No p
↪assword required."
http://prime.worstwestern.com/api/v1/authentication:"Welcome to PrestaShop Webse
↪rvice, please enter the authentication key as the login. No password required.
↪"
http://prime.worstwestern.com/api/v1/folders:"Welcome to PrestaShop Webservice,
↪please enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/v1/status:"Welcome to PrestaShop Webservice, p
↪lease enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/v1/terminal/sessions:"Welcome to PrestaShop We
↪bservice, please enter the authentication key as the login. No password requir
↪ed."
http://prime.worstwestern.com/api/v1/terminal:"Welcome to PrestaShop Webservice,
↪ please enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/v1/users/connection-token:"Welcome to PrestaSh
↪op Webservice, please enter the authentication key as the login. No password r
↪equired."
http://prime.worstwestern.com/api/v1/users:"Welcome to PrestaShop Webservice, pl
↪ease enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/v1:"Welcome to PrestaShop Webservice, please e
↪nter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/v2.0:"Welcome to PrestaShop Webservice, please
↪ enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/v2:"Welcome to PrestaShop Webservice, please e
↪nter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/v3.0:"Welcome to PrestaShop Webservice, please
↪ enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/v3:"Welcome to PrestaShop Webservice, please e
↪nter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/v4.0:"Welcome to PrestaShop Webservice, please
↪ enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/v4/teams:"Welcome to PrestaShop Webservice, pl
↪ease enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/v4/users/me/teams:"Welcome to PrestaShop Webse
↪rvice, please enter the authentication key as the login. No password required.
↪"
http://prime.worstwestern.com/api/v4/users/me:"Welcome to PrestaShop Webservice,
↪ please enter the authentication key as the login. No password required."
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
http://prime.worstwestern.com/api/v4/users:"Welcome to PrestaShop Webservice, pl
↪ease enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/v4:"Welcome to PrestaShop Webservice, please e
↪nter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/v5.0:"Welcome to PrestaShop Webservice, please
↪ enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/v5:"Welcome to PrestaShop Webservice, please e
↪nter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/vendor/phpunit/phpunit/src/Util/PHP:"Welcome t
↪o PrestaShop Webservice, please enter the authentication key as the login. No
↪password required."
http://prime.worstwestern.com/api/vendor/phpunit/phpunit/src/Util:"Welcome to Pr
↪estaShop Webservice, please enter the authentication key as the login. No pass
↪word required."
http://prime.worstwestern.com/api/vendor/phpunit/phpunit/src:"Welcome to PrestaS
↪hop Webservice, please enter the authentication key as the login. No password
↪required."
http://prime.worstwestern.com/api/vendor/phpunit/phpunit:"Welcome to PrestaShop
↪Webservice, please enter the authentication key as the login. No password requ
↪ired."
http://prime.worstwestern.com/api/vendor/phpunit:"Welcome to PrestaShop Webservi
↪ce, please enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/vendor:"Welcome to PrestaShop Webservice, plea
↪se enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api/vppv2:"Welcome to PrestaShop Webservice, pleas
↪e enter the authentication key as the login. No password required."
http://prime.worstwestern.com/api:"Welcome to PrestaShop Webservice, please ente
↪r the authentication key as the login. No password required."
```

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

. . . continues on next page . . .

. . . continued from previous page . . .

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 10.0.2.9]

2.1.2 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection: 80

Vulnerability Detection Result

```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Insight

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: `ICMP Timestamp Reply Information Disclosure`

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: `2023-05-11T09:09:33Z`

References

```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 10.0.2.9]

2.1.3 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: 1406658538
Packet 2: 1406659602
```

Impact

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

Solution:

Solution type: Mitigation

. . . continues on next page . . .

. . . continued from previous page . . .

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
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 10.0.2.9]

This file was automatically generated.