Scan Report

March 21, 2025

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 "Daily scan game servers". The scan started at Thu Mar 20 15:01:29 2025 UTC and ended at Thu Mar 20 17:21:53 2025 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
192.168.112.3	0	1	3	0	0
192.168.112.5	0	1	3	0	0
192.168.112.4	0	1	3	0	0
Total: 3	0	3	9	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 12 results selected by the filtering described above. Before filtering there were 445 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.112.3	SSH	Success	Protocol SSH, Port 22, User student
192.168.112.5	SSH	Success	Protocol SSH, Port 22, User student
192.168.112.4	SSH	Success	Protocol SSH, Port 22, User student

2 Results per Host

2.1 192.168.112.3

Host scan start Thu Mar 20 15:01:54 2025 UTC
Host scan end Thu Mar 20 17:20:04 2025 UTC

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

2.1.1 Medium 80/tcp

Medium (CVSS: 5.3)
NVT: WordPress < 6.5 Private Information Exposure Vulnerability

Summary
WordPress is prone to a private information exposure via 'redirect_guess_404_permalink()'.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 6.1.1
Fixed version:     6.5
Installation
path / port:       /
```

Impact
This can allow unauthenticated attackers to expose the slug of a custom post whose 'publicly_queryable' post status has been set to 'false'.

Solution:
Solution type: VendorFix
Update to version 6.5 or later.
Note: As of 04/2024 the security fix is only available in version 6.5 and haven't been 'backported' to older versions yet.

Affected Software/OS
WordPress versions prior to 6.5.

Vulnerability Insight
When guessing the proper URL to redirect a 404, WordPress only considers the post statuses and not the proper post type privacy settings, leading to potential information disclosure.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress < 6.5 Private Information Exposure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.114477
Version used: `2025-01-13T08:32:03Z`

References
```
cve: CVE-2023-5692
url: https://core.trac.wordpress.org/ticket/59795
url: https://core.trac.wordpress.org/changeset/57645
url: https://bugzilla.redhat.com/show_bug.cgi?id=2273662
url: https://www.wordfence.com/threat-intel/vulnerabilities/id/6e6f993b-ce09-405
↪0-84a1-cbe9953f36b1
```

... continues on next page ...

... continued from previous page ...

```
url: https://patchstack.com/database/vulnerability/wordpress/wordpress-wordpress
↪-core-plugin-6-4-3-sensitive-information-exposure-via-redirect-guess-404-perma
↪link-vulnerability
cert-bund: WID-SEC-2024-0808
```

[return to 192.168.112.3]

2.1.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

Product detection result

```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

Summary

The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

Solution:

Solution type: Mitigation

Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method

Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.

Currently weak MAC algorithms are defined as the following:

- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm

... continues on next page ...

... continued from previous page ...

Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

References
`url: https://www.rfc-editor.org/rfc/rfc6668`
`url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4`

[return to 192.168.112.3]

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 (QoD): 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: 3208196490
Packet 2: 3208197512
```

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.

... continues on next page ...

... continued from previous page ...

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 192.168.112.3]

2.1.4 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 (QoD): 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

... continues on next page ...

... continued from previous page ...

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)

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: `2025-01-21T05:37:33Z`

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 192.168.112.3]

2.2 192.168.112.5

Host scan start	Thu Mar 20 15:01:54 2025 UTC
Host scan end	Thu Mar 20 17:21:48 2025 UTC

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

2.2.1 Medium 80/tcp

Medium (CVSS: 5.3)
NVT: WordPress < 6.5 Private Information Exposure Vulnerability

... continues on next page ...

... continued from previous page ...

Summary
WordPress is prone to a private information exposure via 'redirect_guess_404_permalink()'.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 6.1.1
Fixed version:     6.5
Installation
path / port:       /
```

Impact
This can allow unauthenticated attackers to expose the slug of a custom post whose 'publicly_queryable' post status has been set to 'false'.

Solution:
Solution type: VendorFix
Update to version 6.5 or later.
Note: As of 04/2024 the security fix is only available in version 6.5 and haven't been 'backported' to older versions yet.

Affected Software/OS
WordPress versions prior to 6.5.

Vulnerability Insight
When guessing the proper URL to redirect a 404, WordPress only considers the post statuses and not the proper post type privacy settings, leading to potential information disclosure.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress < 6.5 Private Information Exposure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.114477
Version used: `2025-01-13T08:32:03Z`

References
```
cve: CVE-2023-5692
url: https://core.trac.wordpress.org/ticket/59795
url: https://core.trac.wordpress.org/changeset/57645
url: https://bugzilla.redhat.com/show_bug.cgi?id=2273662
url: https://www.wordfence.com/threat-intel/vulnerabilities/id/6e6f993b-ce09-405
↪0-84a1-cbe9953f36b1
url: https://patchstack.com/database/vulnerability/wordpress/wordpress-wordpress
↪-core-plugin-6-4-3-sensitive-information-exposure-via-redirect-guess-404-perma
↪link-vulnerability
cert-bund: WID-SEC-2024-0808
```

[return to 192.168.112.5]

2.2.2 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 (QoD): 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)

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: `2025-01-21T05:37:33Z`

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 192.168.112.5]

2.2.3 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

Product detection result
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)

Summary
The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote SSH server supports the following weak client-to-server MAC algorithm(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm(s):
umac-64-etm@openssh.com
umac-64@openssh.com

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

... continues on next page ...

... continued from previous page ...

References
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[return to 192.168.112.5]

2.2.4 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 (QoD): 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: 3638381117
Packet 2: 3638382133

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

... continues on next page ...

... continued from previous page ...

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 192.168.112.5]

2.3 192.168.112.4

Host scan start Thu Mar 20 15:01:54 2025 UTC
Host scan end Thu Mar 20 17:21:25 2025 UTC

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

2.3.1 Medium 80/tcp

Medium (CVSS: 5.3)
NVT: WordPress < 6.5 Private Information Exposure Vulnerability

Summary
WordPress is prone to a private information exposure via 'redirect_guess_404_permalink()'.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Installed version: 6.1.1`
`Fixed version: 6.5`
`Installation`
`path / port: /`

Impact

... continues on next page ...

... continued from previous page ...

This can allow unauthenticated attackers to expose the slug of a custom post whose 'publicly_queryable' post status has been set to 'false'.

Solution:
Solution type: VendorFix
Update to version 6.5 or later.
Note: As of 04/2024 the security fix is only available in version 6.5 and haven't been 'backported' to older versions yet.

Affected Software/OS
WordPress versions prior to 6.5.

Vulnerability Insight
When guessing the proper URL to redirect a 404, WordPress only considers the post statuses and not the proper post type privacy settings, leading to potential information disclosure.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `WordPress < 6.5 Private Information Exposure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.114477
Version used: `2025-01-13T08:32:03Z`

References
`cve: CVE-2023-5692`
`url: https://core.trac.wordpress.org/ticket/59795`
`url: https://core.trac.wordpress.org/changeset/57645`
`url: https://bugzilla.redhat.com/show_bug.cgi?id=2273662`
`url: https://www.wordfence.com/threat-intel/vulnerabilities/id/6e6f993b-ce09-405`
`↪0-84a1-cbe9953f36b1`
`url: https://patchstack.com/database/vulnerability/wordpress/wordpress-wordpress`
`↪-core-plugin-6-4-3-sensitive-information-exposure-via-redirect-guess-404-perma`
`↪link-vulnerability`
`cert-bund: WID-SEC-2024-0808`

[return to 192.168.112.4]

2.3.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: Weak MAC Algorithm(s) Supported (SSH)

Product detection result
`cpe:/a:ietf:secure_shell_protocol`
`Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565`
`↪)`

... continues on next page ...

... continued from previous page ...

Summary
The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

References
```
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4
```

[return to 192.168.112.4]

2.3.3 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 (QoD): 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)

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: `2025-01-21T05:37:33Z`

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 192.168.112.4]

2.3.4 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 (QoD): 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: 3086775734
Packet 2: 3086776754
```

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
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 192.168.112.4]

This file was automatically generated.