

Scan Report

October 7, 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 “Docker-containers”. The scan started at Mon Oct 7 19:10:40 2024 UTC and ended at Mon Oct 7 19:14:06 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	2
2	Results per Host	2
2.1	192.168.100.204	2
	2.1.1 Low general/icmp	2
2.2	192.168.100.202	3
	2.2.1 Low general/icmp	4
2.3	192.168.100.203	5
	2.3.1 Low general/icmp	5
2.4	192.168.100.201	6
	2.4.1 Low general/icmp	6

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.100.204	0	0	1	0	0
192.168.100.202	0	0	1	0	0
192.168.100.203	0	0	1	0	0
192.168.100.201	0	0	1	0	0
Total: 4	0	0	4	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 4 results selected by the filtering described above. Before filtering there were 24 results.

2 Results per Host

2.1 192.168.100.204

Host scan start Mon Oct 7 19:11:23 2024 UTC

Host scan end Mon Oct 7 19:13:57 2024 UTC

Service (Port)	Threat Level
general/icmp	Low

2.1.1 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%
... continues on next page ...

...continued from previous page ...
Vulnerability Detection Result The following response / ICMP packet has been received: <ul style="list-style-type: none">- 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: <ul style="list-style-type: none">- 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: 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 192.168.100.204](#)]

2.2 192.168.100.202

Host scan start Mon Oct 7 19:11:23 2024 UTC
Host scan end Mon Oct 7 19:13:57 2024 UTC

Service (Port)	Threat Level
general/icmp	Low

2.2.1 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: 2023-05-11T09:09:33Z
References cve: CVE-1999-0524 url: https://datatracker.ietf.org/doc/html/rfc792
... continues on next page ...

...continued from previous page ...

url: <https://datatracker.ietf.org/doc/html/rfc2780>
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658

[\[return to 192.168.100.202 \]](#)

2.3 192.168.100.203

Host scan start Mon Oct 7 19:11:23 2024 UTC

Host scan end Mon Oct 7 19:13:59 2024 UTC

Service (Port)	Threat Level
general/icmp	Low

2.3.1 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

... continues on next page ...

...continued from previous page ...

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

[\[return to 192.168.100.203 \]](#)

2.4 192.168.100.201

Host scan start Mon Oct 7 19:11:23 2024 UTC

Host scan end Mon Oct 7 19:13:58 2024 UTC

Service (Port)	Threat Level
general/icmp	Low

2.4.1 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

... continues on next page ...

...continued from previous page...

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: 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 192.168.100.201](#)]