# Scan Report

June 18, 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 "Iot_target". The scan started at Tue Jun 18 20:52:58 2024 UTC and ended at Tue Jun 18 20:59:49 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 |
|---|---|---|---|---|---|
| 192.168.14.240 _gateway | 0 | 2 | 2 | 0 | 0 |
| Total: 1 | 0 | 2 | 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 4 results selected by the filtering described above. Before filtering there were 32 results.

# 2 Results per Host

## 2.1 192.168.14.240

| | |
|---|---|
| Host scan start | Tue Jun 18 20:53:49 2024 UTC |
| Host scan end | Tue Jun 18 20:59:42 2024 UTC |

| Service (Port) | Threat Level |
|---|---|
| 53/udp | Medium |
| 1883/tcp | Medium |
| general/tcp | Low |
| general/icmp | Low |

### 2.1.1 Medium 53/udp

Medium (CVSS: 5.0)

NVT: DNS Cache Snooping Vulnerability (UDP) - Active Check

**Summary**
The DNS server is prone to a cache snooping vulnerability.

. . . continues on next page . . .

... continued from previous page ...

**Quality of Detection:** 70

**Vulnerability Detection Result**
`Received (an) answer(s) for a non-recursive query for "example.com".`
`Result:`
`93.184.215.14`

**Impact**
Attackers might gain information about cached DNS records which might lead to further attacks.
Note: This finding might be an acceptable risk if you:
- trust all clients which can reach the server
- do not allow recursive queries from outside your trusted client network.

**Solution:**
**Solution type:** Mitigation
There are multiple possible mitigation steps depending on location and functionality needed by the DNS server:
- Disable recursion
- Don't allow public access to DNS Servers doing recursion
- Leave recursion enabled if the DNS Server stays on a corporate network that cannot be reached by untrusted clients

**Vulnerability Insight**
DNS cache snooping is when someone queries a DNS server in order to find out (snoop) if the DNS server has a specific DNS record cached, and thereby deduce if the DNS server's owner (or its users) have recently visited a specific site.
This may reveal information about the DNS server's owner, such as what vendor, bank, service provider, etc. they use. Especially if this is confirmed (snooped) multiple times over a period.
This method could even be used to gather statistical information - for example at what time does the DNS server's owner typically access his net bank etc. The cached DNS record's remaining TTL value can provide very accurate data for this.
DNS cache snooping is possible even if the DNS server is not configured to resolve recursively for 3rd parties, as long as it provides records from the cache also to 3rd parties (a.k.a. 'lame requests').

**Vulnerability Detection Method**
Sends a crafted DNS query and checks the response.
Details: `DNS Cache Snooping Vulnerability (UDP) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.146591
Version used: `2023-03-24T10:19:42Z`

**References**
`url: https://www.cs.unc.edu/~fabian/course_papers/cache_snooping.pdf`
`url: https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/dns`
`↪-server-cache-snooping-attacks`

... continues on next page ...

... continued from previous page ...

url: https://kb.isc.org/docs/aa-00509
url: https://kb.isc.org/docs/aa-00482

[ return to 192.168.14.240 ]

### 2.1.2 Medium 1883/tcp

Medium (CVSS: 6.4)

NVT: MQTT Broker Does Not Require Authentication

**Summary**
The remote MQTT broker does not require authentication.

**Quality of Detection:** 80

**Vulnerability Detection Result**
Vulnerability was detected according to the Vulnerability Detection Method.

**Solution:**
**Solution type:** Mitigation
Enable authentication.

**Vulnerability Detection Method**
Checks if authentication is required for the remote MQTT broker.
Details: MQTT Broker Does Not Require Authentication
OID:1.3.6.1.4.1.25623.1.0.140167
Version used: 2022-07-11T10:16:03Z

**References**
url: https://www.heise.de/newsticker/meldung/MQTT-Protokoll-IoT-Kommunikation-vo
↪n-Reaktoren-und-Gefaengnissen-oeffentlich-einsehbar-3629650.html

[ return to 192.168.14.240 ]

### 2.1.3 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

**Summary**

... continues on next page ...

... continued from previous page ...

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: 892492599
Packet 2: 892493685
```

**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 192.168.14.240 ]

### 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:** 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
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 192.168.14.240 ]

---