Scan Report

August 14, 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 "Lausanne scan". The scan started at Mon Aug 12 11:18:28 2024 UTC and ended at Mon Aug 12 11:47:12 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
192.168.112.1	1	6	3	0	0
Total: 1	1	6	3	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 10 results selected by the filtering described above. Before filtering there were 123 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.112.1	SSH	Success	Protocol SSH, Port 22, User scion

2 Results per Host

2.1 192.168.112.1

Host scan start Mon Aug 12 11:18:56 2024 UTC
Host scan end Mon Aug 12 11:47:03 2024 UTC

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

2.1.1 High package

High (CVSS: 8.1)

NVT: Ubuntu: Security Advisory (USN-6473-2)

Summary
The remote host is missing an update for the 'python-pip' package(s) announced via the USN-6473-2 advisory.

Quality of Detection (QoD): 97%

Vulnerability Detection Result
```
Vulnerable package:   python3-pip
Installed version:    python3-pip-22.0.2+dfsg-1ubuntu0.3
Fixed version:      >=python3-pip-22.0.2+dfsg-1ubuntu0.4
```

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'python-pip' package(s) on Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.04, Ubuntu 23.10.

Vulnerability Insight
USN-6473-1 fixed vulnerabilities in urllib3. This update provides the corresponding updates for the urllib3 module bundled into pip.
Original advisory details:
It was discovered that urllib3 didn't strip HTTP Authorization header on cross-origin redirects. A remote attacker could possibly use this issue to obtain sensitive information. This issue only affected Ubuntu 16.04 LTS and Ubuntu 18.04 LTS. (CVE-2018-25091)
It was discovered that urllib3 didn't strip HTTP Cookie header on cross-origin redirects. A remote attacker could possibly use this issue to obtain sensitive information. (CVE-2023-43804)
It was discovered that urllib3 didn't strip HTTP body on status code 303 redirects under certain circumstances. A remote attacker could possibly use this issue to obtain sensitive information. (CVE-2023-45803)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6473-2)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6473.2
Version used: `2024-02-02T04:09:01Z`

References
```
url: https://ubuntu.com/security/notices/USN-6473-2
cve: CVE-2018-25091
cve: CVE-2023-43804
```

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2023-45803
advisory_id: USN-6473-2
cert-bund: WID-SEC-2024-1228
cert-bund: WID-SEC-2024-1003
cert-bund: WID-SEC-2024-0794
cert-bund: WID-SEC-2024-0423
cert-bund: WID-SEC-2023-3146
cert-bund: WID-SEC-2023-3025
cert-bund: WID-SEC-2023-2964
cert-bund: WID-SEC-2023-2862
dfn-cert: DFN-CERT-2024-1392
dfn-cert: DFN-CERT-2024-1391
dfn-cert: DFN-CERT-2024-1384
dfn-cert: DFN-CERT-2024-1382
dfn-cert: DFN-CERT-2024-1380
dfn-cert: DFN-CERT-2024-0744
dfn-cert: DFN-CERT-2024-0598
dfn-cert: DFN-CERT-2024-0312
dfn-cert: DFN-CERT-2024-0073
dfn-cert: DFN-CERT-2023-3204
dfn-cert: DFN-CERT-2023-3160
dfn-cert: DFN-CERT-2023-2914
dfn-cert: DFN-CERT-2023-2724
dfn-cert: DFN-CERT-2023-2714
dfn-cert: DFN-CERT-2023-2563
dfn-cert: DFN-CERT-2023-2421
dfn-cert: DFN-CERT-2023-2366
```

[return to 192.168.112.1]

2.1.2 Medium package

Medium (CVSS: 5.5)

NVT: Ubuntu: Security Advisory (USN-6478-1)

Summary
The remote host is missing an update for the 'traceroute' package(s) announced via the USN-6478-1 advisory.

Quality of Detection (QoD): 97%

Vulnerability Detection Result

```
Vulnerable package:    traceroute
Installed version:     traceroute-1:2.1.0-2
```

... continues on next page ...

... continued from previous page ...

Fixed version: >=traceroute-1:2.1.0-2ubuntu0.22.04.1~esm1

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'traceroute' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight
It was discovered that Traceroute did not properly parse command line arguments. An attacker could possibly use this issue to execute arbitrary commands.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6478-1)
OID:1.3.6.1.4.1.25623.1.1.12.2023.6478.1
Version used: 2024-02-02T04:09:01Z

References
url: https://ubuntu.com/security/notices/USN-6478-1
cve: CVE-2023-46316
advisory_id: USN-6478-1
cert-bund: WID-SEC-2024-1208
dfn-cert: DFN-CERT-2023-2235

Medium (CVSS: 5.5)

NVT: Ubuntu: Security Advisory (USN-6640-1)

Summary
The remote host is missing an update for the 'shadow' package(s) announced via the USN-6640-1 advisory.

Quality of Detection (QoD): 97%

Vulnerability Detection Result
Vulnerable package: login
Installed version: login-1:4.8.1-2ubuntu2.1
Fixed version: >=login-1:4.8.1-2ubuntu2.2

Solution:
Solution type: VendorFix
Please install the updated package(s).

... continues on next page ...

... continued from previous page ...

Affected Software/OS
'shadow' package(s) on Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04, Ubuntu 20.04, Ubuntu 22.04, Ubuntu 23.10.

Vulnerability Insight
It was discovered that shadow was not properly sanitizing memory when running the password utility. An attacker could possibly use this issue to retrieve a password from memory, exposing sensitive information.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6640-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6640.1
Version used: `2024-02-16T04:08:40Z`

References
```
url: https://ubuntu.com/security/notices/USN-6640-1
cve: CVE-2023-4641
advisory_id: USN-6640-1
cert-bund: WID-SEC-2024-1307
cert-bund: WID-SEC-2024-0869
cert-bund: WID-SEC-2023-3146
cert-bund: WID-SEC-2023-2357
dfn-cert: DFN-CERT-2024-1092
dfn-cert: DFN-CERT-2024-0818
dfn-cert: DFN-CERT-2023-3124
dfn-cert: DFN-CERT-2023-2141
```

Medium (CVSS: 5.0)

NVT: Ubuntu: Security Advisory (USN-6937-1)

Summary
The remote host is missing an update for the 'openssl' package(s) announced via the USN-6937-1 advisory.

Quality of Detection (QoD): 97%

Vulnerability Detection Result
```
Vulnerable package:   libssl3
Installed version:    libssl3-3.0.2-0ubuntu1.16
Fixed version:      >=libssl3-3.0.2-0ubuntu1.17
```

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'openssl' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 24.04.

Vulnerability Insight
It was discovered that OpenSSL incorrectly handled TLSv1.3 sessions when certain non-default TLS server configurations were in use. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, leading to a denial of service. (CVE-2024-2511)
It was discovered that OpenSSL incorrectly handled checking excessively long DSA keys or parameters. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, leading to a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 24.04 LTS. (CVE-2024-4603)
William Ahern discovered that OpenSSL incorrectly handled certain memory operations in a rarely-used API. A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2024-4741)
Joseph Birr-Pixton discovered that OpenSSL incorrectly handled calling a certain API with an empty supported client protocols buffer. A remote attacker could possibly use this issue to obtain sensitive information, or cause OpenSSL to crash, resulting in a denial of service. (CVE-2024-5535)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6937-1)`
OID:1.3.6.1.4.1.25623.1.1.12.2024.6937.1
Version used: `2024-08-01T04:08:31Z`

References
`url: https://ubuntu.com/security/notices/USN-6937-1`
`cve: CVE-2024-2511`
`cve: CVE-2024-4603`
`cve: CVE-2024-4741`
`cve: CVE-2024-5535`
`advisory_id: USN-6937-1`
`cert-bund: WID-SEC-2024-1645`
`cert-bund: WID-SEC-2024-1638`
`cert-bund: WID-SEC-2024-1469`
`cert-bund: WID-SEC-2024-1240`
`cert-bund: WID-SEC-2024-1171`
`cert-bund: WID-SEC-2024-0813`
`dfn-cert: DFN-CERT-2024-1978`
`dfn-cert: DFN-CERT-2024-1968`
`dfn-cert: DFN-CERT-2024-1904`
`dfn-cert: DFN-CERT-2024-1867`
`dfn-cert: DFN-CERT-2024-1851`

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2024-1681
dfn-cert: DFN-CERT-2024-1587
dfn-cert: DFN-CERT-2024-1493
dfn-cert: DFN-CERT-2024-1423
dfn-cert: DFN-CERT-2024-1330
dfn-cert: DFN-CERT-2024-0916

Medium (CVSS: 5.0)

NVT: Ubuntu: Security Advisory (USN-6431-3)

Summary
The remote host is missing an update for the 'iperf3' package(s) announced via the USN-6431-3 advisory.

Quality of Detection (QoD): 97%

Vulnerability Detection Result

```
Vulnerable package:   iperf3
Installed version:    iperf3-3.9-1+deb11u1build0.22.04.1
Fixed version:      >=iperf3-3.9-1+deb11u1ubuntu0.1~esm1
Vulnerable package:   libiperf0
Installed version:    libiperf0-3.9-1+deb11u1build0.22.04.1
Fixed version:      >=libiperf0-3.9-1+deb11u1ubuntu0.1~esm1
```

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'iperf3' package(s) on Ubuntu 22.04.

Vulnerability Insight
USN-6431-1 fixed a vulnerability in iperf3. This update provides the corresponding update for Ubuntu 22.04 LTS.
Original advisory details:
Jorge Sancho Larraz discovered that iperf3 did not properly manage certain inputs, which could cause the server process to stop responding, waiting for input on the control connection. A remote attacker could possibly use this issue to cause a denial of service. (LP: #2038654)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Ubuntu: Security Advisory (USN-6431-3)`
OID:1.3.6.1.4.1.25623.1.1.12.2023.6431.3

... continues on next page ...

... continued from previous page ...

Version used: 2023-10-17T04:08:26Z

References
url: https://ubuntu.com/security/notices/USN-6431-3
url: https://launchpad.net/bugs/2038654
advisory_id: USN-6431-3

Medium (CVSS: 5.0)

NVT: Ubuntu: Security Advisory (USN-6944-1)

Summary
The remote host is missing an update for the 'curl' package(s) announced via the USN-6944-1 advisory.

Quality of Detection (QoD): 97%

Vulnerability Detection Result
```
Vulnerable package:   curl
Installed version:    curl-7.81.0-1ubuntu1.16
Fixed version:      >=curl-7.81.0-1ubuntu1.17
Vulnerable package:   libcurl3-gnutls
Installed version:    libcurl3-gnutls-7.81.0-1ubuntu1.16
Fixed version:      >=libcurl3-gnutls-7.81.0-1ubuntu1.17
Vulnerable package:   libcurl4
Installed version:    libcurl4-7.81.0-1ubuntu1.16
Fixed version:      >=libcurl4-7.81.0-1ubuntu1.17
```

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'curl' package(s) on Ubuntu 20.04, Ubuntu 22.04, Ubuntu 24.04.

Vulnerability Insight
Dov Murik discovered that curl incorrectly handled parsing ASN.1 Generalized Time fields. A remote attacker could use this issue to cause curl to crash, resulting in a denial of service, or possibly obtain sensitive memory contents.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Ubuntu: Security Advisory (USN-6944-1)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6944.1

... continues on next page ...

... continued from previous page ...

Version used: 2024-08-06T04:09:11Z

References
url: https://ubuntu.com/security/notices/USN-6944-1
cve: CVE-2024-7264
advisory_id: USN-6944-1
cert-bund: WID-SEC-2024-1736
dfn-cert: DFN-CERT-2024-2025
dfn-cert: DFN-CERT-2024-1967

Medium (CVSS: 5.0)

NVT: Ubuntu: Security Advisory (USN-6928-1)

Summary
The remote host is missing an update for the 'python3.8, python3.10' package(s) announced via the USN-6928-1 advisory.

Quality of Detection (QoD): 97%

Vulnerability Detection Result
```
Vulnerable package:   python3.10
Installed version:    python3.10-3.10.12-1~22.04.4
Fixed version:      >=python3.10-3.10.12-1~22.04.5
Vulnerable package:   python3.10-minimal
Installed version:    python3.10-minimal-3.10.12-1~22.04.4
Fixed version:      >=python3.10-minimal-3.10.12-1~22.04.5
```

Solution:
Solution type: VendorFix
Please install the updated package(s).

Affected Software/OS
'python3.8, python3.10' package(s) on Ubuntu 20.04, Ubuntu 22.04.

Vulnerability Insight
It was discovered that the Python ssl module contained a memory race condition when handling the APIs to obtain the CA certificates and certificate store statistics. This could possibly result in applications obtaining wrong results, leading to various SSL issues. (CVE-2024-0397)
It was discovered that the Python ipaddress module contained incorrect information about which IP address ranges were considered 'private' or 'globally reachable'. This could possibly result in applications applying incorrect security policies. (CVE-2024-4032)

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.

... continues on next page ...

... continued from previous page ...

Details: Ubuntu: Security Advisory (USN-6928-1)
OID:1.3.6.1.4.1.25623.1.1.12.2024.6928.1
Version used: 2024-07-31T04:07:34Z

References

url: https://ubuntu.com/security/notices/USN-6928-1
cve: CVE-2024-0397
cve: CVE-2024-4032
advisory_id: USN-6928-1
cert-bund: WID-SEC-2024-1645
cert-bund: WID-SEC-2024-1396
dfn-cert: DFN-CERT-2024-1908
dfn-cert: DFN-CERT-2024-1851
dfn-cert: DFN-CERT-2024-1833
dfn-cert: DFN-CERT-2024-1702
dfn-cert: DFN-CERT-2024-1615

[return to 192.168.112.1]

2.1.3 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

... continues on next page ...

... continued from previous page ...

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 192.168.112.1]

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
```

... 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 192.168.112.1]

2.1.5 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%

... continues on next page ...

... continued from previous page ...

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: 2569131963
Packet 2: 2569133061

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 192.168.112.1]