Scan Report

February 7, 2026

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 "Ubuntu Auth Scan". The scan started at Fri Feb 6 16:41:59 2026 UTC and ended at Fri Feb 6 17:00:27 2026 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**

1.1 Host Authentications 2

2 Results per Host **2**

2.1 192.168.186.131 2

2.1.1 Medium general/tcp 2

2.1.2 Low 22/tcp 5

2.1.3 Low general/tcp 6

2.1.4 Low general/icmp 9

1 Result Overview

Host	Critical	High	Medium	Low	Log	False P.
192.168.186.131	0	0	1	4	0	0
Total: 1	0	0	1	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 5 results selected by the filtering described above. Before filtering there were 239 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.186.131	SSH	Success	Protocol SSH, Port 22, User agent

2 Results per Host

2.1 192.168.186.131

Host scan start	Fri Feb 6 16:42:41 2026 UTC
Host scan end	Fri Feb 6 17:00:21 2026 UTC

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

2.1.1 Medium general/tcp

Medium (CVSS: 4.6)

NVT: Missing Linux Kernel mitigations for 'Register File Data Sampling (RFDS)' hardware vulnerability (INTEL-SA-00898)

Product detection result

```
cpe:/a:linux:kernel
Detected by Detection of Linux Kernel mitigation status for hardware vulnerabili
↪ties (OID: 1.3.6.1.4.1.25623.1.0.108765)
```

Summary

The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'Register File Data Sampling (RFDS)' hardware vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The Linux Kernel on the remote host is missing the mitigation for the "reg_file_
↪data_sampling" hardware vulnerability as reported by the sysfs interface:
sysfs file checked                                             | Linux Kernel st
↪atus (SSH response)
--------------------------------------------------------------------------------
↪-------------------
/sys/devices/system/cpu/vulnerabilities/reg_file_data_sampling | Vulnerable: No
↪microcode
Notes on the "Linux Kernel status (SSH response)" column:
- sysfs file missing: The sysfs interface is available but the sysfs file for th
↪is specific vulnerability is missing. This means the current Linux Kernel does
↪n't know this vulnerability yet. Based on this it is assumed that it doesn't p
↪rovide any mitigation and that the target system is vulnerable.
- Strings including "Mitigation:", "Not affected" or "Vulnerable" are reported d
↪irectly by the Linux Kernel.
- All other strings are responses to various SSH commands.
```

Solution:

Solution type: VendorFix

The following solutions exist:
- Update to a more recent Linux Kernel to receive mitigations on Kernel level and info about the mitigation status from it
- Enable the mitigation(s) in the Linux Kernel (might be disabled depending on the configuration)

Additional possible mitigations (if provided by the vendor) are to:
- install a Microcode update
- update the BIOS of the Mainboard

Note: Please create an override for this result if one of the following applies:
- the sysfs file is not available but other mitigations like a Microcode update is already in place
- the sysfs file is not available but the CPU of the host is not affected

. . . continues on next page . . .

. . . continued from previous page . . .

- the reporting of the Linux Kernel is not correct (this is out of the control of this VT)

Affected Software/OS

Various Intel CPUs. Please see the references for the full list of affected CPUs.

Vulnerability Detection Method

Checks previous gathered information on the mitigation status reported by the Linux Kernel.
Details: `Missing Linux Kernel mitigations for 'Register File Data Sampling (RFDS)' hardw.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.114456
Version used: `2025-05-16T05:40:21Z`

Product Detection Result

Product: `cpe:/a:linux:kernel`
Method: `Detection of Linux Kernel mitigation status for hardware vulnerabilities`
OID: 1.3.6.1.4.1.25623.1.0.108765)

References

```
cve: CVE-2023-28746
url: https://docs.kernel.org/admin-guide/hw-vuln/reg-file-data-sampling.html
url: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-0
↪0898.html
url: https://www.intel.com/content/www/us/en/developer/topic-technology/software
↪-security-guidance/processors-affected-consolidated-product-cpu-model.html
url: https://www.intel.com/content/www/us/en/developer/articles/technical/softwa
↪re-security-guidance/advisory-guidance/register-file-data-sampling.html
cert-bund: WID-SEC-2025-0794
cert-bund: WID-SEC-2024-1913
cert-bund: WID-SEC-2024-0619
cert-bund: WID-SEC-2024-0615
dfn-cert: DFN-CERT-2025-2802
dfn-cert: DFN-CERT-2025-2291
dfn-cert: DFN-CERT-2025-0933
dfn-cert: DFN-CERT-2025-0774
dfn-cert: DFN-CERT-2024-3416
dfn-cert: DFN-CERT-2024-2999
dfn-cert: DFN-CERT-2024-2750
dfn-cert: DFN-CERT-2024-2748
dfn-cert: DFN-CERT-2024-2175
dfn-cert: DFN-CERT-2024-2173
dfn-cert: DFN-CERT-2024-2033
dfn-cert: DFN-CERT-2024-1850
dfn-cert: DFN-CERT-2024-1448
dfn-cert: DFN-CERT-2024-1444
dfn-cert: DFN-CERT-2024-1309
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2024-1304
dfn-cert: DFN-CERT-2024-1202
dfn-cert: DFN-CERT-2024-1173
dfn-cert: DFN-CERT-2024-1122
dfn-cert: DFN-CERT-2024-1039
dfn-cert: DFN-CERT-2024-1024
dfn-cert: DFN-CERT-2024-1023
dfn-cert: DFN-CERT-2024-0986
dfn-cert: DFN-CERT-2024-0910
dfn-cert: DFN-CERT-2024-0780
dfn-cert: DFN-CERT-2024-0773
dfn-cert: DFN-CERT-2024-0772
dfn-cert: DFN-CERT-2024-0771
dfn-cert: DFN-CERT-2024-0770
dfn-cert: DFN-CERT-2024-0708
dfn-cert: DFN-CERT-2024-0690
dfn-cert: DFN-CERT-2024-0689
dfn-cert: DFN-CERT-2024-0678
dfn-cert: DFN-CERT-2024-0666
dfn-cert: DFN-CERT-2024-0665
dfn-cert: DFN-CERT-2024-0628
```

[return to 192.168.186.131]

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
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
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 192.168.186.131]

2.1.3 Low general/tcp

Low (CVSS: 3.8)

NVT: Missing Linux Kernel mitigations for 'Indirect Target Selection (ITS)' hardware vulnerability (INTEL-SA-01153)

Product detection result
```
cpe:/a:linux:kernel
Detected by Detection of Linux Kernel mitigation status for hardware vulnerabili
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪ties (OID: 1.3.6.1.4.1.25623.1.0.108765)
```

Summary

The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'Indirect Target Selection (ITS)' hardware vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The Linux Kernel on the remote host is missing the mitigation for the "indirect_
↪target_selection" hardware vulnerability as reported by the sysfs interface:
sysfs file checked                                                | Linux Kernel
↪ status (SSH response)
--------------------------------------------------------------------------------
↪-------------------------------------------------------------------------------
↪----------------------------
/sys/devices/system/cpu/vulnerabilities/indirect_target_selection | sysfs file m
↪issing (cat: /sys/devices/system/cpu/vulnerabilities/indirect_target_selection
↪: No such file or directory)
Notes on the "Linux Kernel status (SSH response)" column:
- sysfs file missing: The sysfs interface is available but the sysfs file for th
↪is specific vulnerability is missing. This means the current Linux Kernel does
↪n't know this vulnerability yet. Based on this it is assumed that it doesn't p
↪rovide any mitigation and that the target system is vulnerable.
- Strings including "Mitigation:", "Not affected" or "Vulnerable" are reported d
↪irectly by the Linux Kernel.
- All other strings are responses to various SSH commands.
```

Solution:

Solution type: VendorFix

The following solutions exist:

- Update to a more recent Linux Kernel to receive mitigations on Kernel level and info about the mitigation status from it
- Enable the mitigation(s) in the Linux Kernel (might be disabled depending on the configuration)

Additional possible mitigations (if provided by the vendor) are to:

- install a Microcode update
- update the BIOS of the Mainboard

Note: Please create an override for this result if one of the following applies:

- the sysfs file is not available but other mitigations like a Microcode update is already in place
- the sysfs file is not available but the CPU of the host is not affected
- the reporting of the Linux Kernel is not correct (this is out of the control of this VT)

Affected Software/OS

Various Intel CPUs. Please see the references for the full list of affected CPUs.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Checks previous gathered information on the mitigation status reported by the Linux Kernel.

Details: `Missing Linux Kernel mitigations for 'Indirect Target Selection (ITS)' hardware.`
`↪..`

OID:1.3.6.1.4.1.25623.1.0.119002

Version used: `2025-05-27T05:40:44Z`

Product Detection Result

Product: `cpe:/a:linux:kernel`

Method: `Detection of Linux Kernel mitigation status for hardware vulnerabilities`

OID: 1.3.6.1.4.1.25623.1.0.108765)

References

```
cve: CVE-2024-28956
url: https://docs.kernel.org/admin-guide/hw-vuln/indirect-target-selection.html
url: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-0
↪1153.html
url: https://www.vusec.net/projects/training-solo/
cert-bund: WID-SEC-2025-1905
cert-bund: WID-SEC-2025-1001
dfn-cert: DFN-CERT-2025-3377
dfn-cert: DFN-CERT-2025-3124
dfn-cert: DFN-CERT-2025-2292
dfn-cert: DFN-CERT-2025-2270
dfn-cert: DFN-CERT-2025-1912
dfn-cert: DFN-CERT-2025-1869
dfn-cert: DFN-CERT-2025-1839
dfn-cert: DFN-CERT-2025-1766
dfn-cert: DFN-CERT-2025-1532
dfn-cert: DFN-CERT-2025-1526
dfn-cert: DFN-CERT-2025-1229
dfn-cert: DFN-CERT-2025-1196
```

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:
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Packet 1: 1189491479
Packet 2: 1189492582
```

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 192.168.186.131]

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
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 192.168.186.131]

This file was automatically generated.