CERT-EU

Security Advisory 2025-031

Multiple Vulnerabilities in Fortinet Products

2025-08-13 — v1.0

TLP:CLEAR

History:

- *13/08/2025 — v1.0 – Initial publication*

Summary

On August 12, 2025, Fortinet released security advisories addressing several vulnerabilities, including a critical one **exploited in the wild**, and two high severity ones.

It is recommended updating as soon as possible.

Technical Details

The vulnerability **CVE-2025-25256**, with a CVSS score of 9.8, is due to improper neutralisation of special elements used in an OS command and allows a remote unauthenticated attacker to execute unauthorised code or commands via crafted CLI requests. The vulnerability is known to be exploited in the wild [1].

The vulnerability **CVE-2024-26009**, with a CVSS score of 7.9, is an authentication bypass using an alternate path or channel vulnerability and may allow an unauthenticated attacker to seize control of a managed device via crafted FGFM requests, if the device is managed by a FortiManager, and if the attacker knows that FortiManager's serial number [2].

The vulnerability **CVE-2025-52970**, with a CVSS score of 7.7, is due to improper handling of parameters and allows an unauthenticated remote attacker in possession of non-public information (pertaining to both the device and to the targeted user) to log in as any existing user on the device via a specially crafted request [3].

Affected Products

The vulnerability **CVE-2025-25256** affects the following versions of FortiSIEM:

- 7.3.0 through 7.3.1
- 7.2.0 through 7.2.5
- 7.1.0 through 7.1.7
- 7.0.0 through 7.0.3
- 6.7.0 through 6.7.9
- 6.6, 6.5, 6.4, 6.3, 6.2 and 6.1

- 5.4

The vulnerability **CVE-2024-26009** affects the following versions of FortiWeb:

- 7.6.0 through 7.6.3
- 7.4.0 through 7.4.7
- 7.2.0 through 7.2.10
- 7.0.0 through 7.0.10

The vulnerability **CVE-2025-52970** affects the following versions FortiOS, FortiPAM, FortiProxy and FortSwitch Manager:

- FortiOS 6.4.0 through 6.4.15
- FortiOS 6.2.0 through 6.2.16
- FortiOS 6.0 all versions
- FortiPAM 1.2 all versions
- FortiPAM 1.1 all versions
- FortiPAM 1.0 all versions
- FortiProxy 7.4.0 through 7.4.2
- FortiProxy 7.2.0 through 7.2.8
- FortiProxy 7.0.0 through 7.0.15
- FortiSwitchManager 7.2.0 through 7.2.3
- FortiSwitchManager 7.0.0 through 7.0.3

Recommendations

It is recommended updating vulnerable products as soon as possible.

Workaround

To mitigate the vulnerability **CVE-2025-25256**, it is possible to limit access to the `phMonitor` port (7900) of FortiSIEM.

References

[1] https://www.fortiguard.com/psirt/FG-IR-25-152

[2] https://www.fortiguard.com/psirt/FG-IR-24-042

[3] https://www.fortiguard.com/psirt/FG-IR-25-448