Security Advisory 2024-017

Critical Vulnerabilites in FortiSIEM

February 6, 2024 — v1.0

TLP:CLEAR

History:

- *06/02/2024 — v1.0 – Initial publication*

Summary

In February 2024, Fortinet quietly updated a 2023 advisory [1], joining two critical flows to the list of OS Command vulnerabilities affecting its FortiSIEM product. If exploited, these vulnerabilities could allow a remote unauthenticated attacker to execute commands on the system.

Updating is recommended as soon as possible.

Technical Details

The vulnerabilities **CVE-2024-23108** and **CVE-2024-23109**, both with a provisional **CVSS score of 10 out of 10**, are due to improper neutralisation of special elements. By sending crafted API requests, a remote unauthenticated attacker could execute commands on the affected system.

On October 10, 2023, Fortinet released the initial version of the advisory regarding a similar vulnerability tracked as **CVE-2023-34992** with a **CVSS score 9.7**.

Affected Products

The following product versions are affected:

- version 7.1.0 through 7.1.1 (fixed in 7.1.2);
- version 7.0.0 through 7.0.2 (fixed in 7.0.3);
- version 6.7.0 through 6.7.8 (fixed in 6.7.9);
- version 6.6.0 through 6.6.3 (fixed in 6.6.5);
- version 6.5.0 through 6.5.2 (fixed in 6.5.3);
- version 6.4.0 through 6.4.2 (fixed in 6.4.4).

Recommendations

CERT-EU recommends upgrading to a non-vulnerable version of the product.

References

[1] https://www.fortiguard.com/psirt/FG-IR-23-130