Security Advisory 2023-092

Critical vulnerability in FortiSIEM

November 21, 2023 — v1.1

TLP:CLEAR

History:

- *20/11/2023 — v1.0 – Initial publication*
- *21/11/2023 — v1.1 – Correction of the CVE ID*

Summary

On November 14, Fortinet released an advisory regarding a critical vulnerability affecting FortiSIEM which may allow a remote unauthenticated attacker to execute unauthorised commands via crafted API requests [1].

Technical Details

The vulnerability `CVE-2023-36553`, with a CVSS score of 9.3 out of 10, is due to an improper neutralisation of special elements in FortiSIEM report server. The exploitation of this vulnerability by a remote unauthenticated attacker could lead to the execution of unauthorised commands via crafted API requests.

Affected Products

This vulnerability affects:

- FortiSIEM 5.4 all versions;
- FortiSIEM 5.3 all versions;
- FortiSIEM 5.2 all versions;
- FortiSIEM 5.1 all versions;
- FortiSIEM 5.0 all versions;
- FortiSIEM 4.10 all versions;
- FortiSIEM 4.9 all versions;
- FortiSIEM 4.7 all versions.

Recommendations

It is recommended updating as soon as possible [1].

References

[1] https://www.fortiguard.com/psirt/FG-IR-23-135