CERT-EU

Security Advisory 2024-006

High Vulnerability in FortiOS & FortiProxy

January 11, 2024 — v1.0

TLP:CLEAR

History:

- *11/01/2024 — v1.0 – Initial publication*

Summary

On January 9, 2024, Fortinet disclosed a high vulnerability in FortiOS & FortiProxy. This vulnerability, tracked as `CVE-2023-44250` and with a CVSS score of 8.3, could allow an authenticated attacker to perform elevated actions via crafted HTTP or HTTPS requests.

Technical Details

The bug is due to an improper privilege management vulnerability in a FortiOS & FortiProxy HA cluster. If exploited, this vulnerability could allow an authenticated attacker to perform elevated actions via crafted HTTP or HTTPS requests.

Affected products

The following versions are affected:

- FortiOS 7.4, from 7.4.0 through 7.4.1;
- FortiOS 7.2.5;
- FortiProxy 7.4, from 7.4.0 through 7.4.1;

Recommendations

CERT-EU recommends upgrading as soon as possible to a fixed version.

References

[1] https://www.fortiguard.com/psirt/FG-IR-23-315