CERT-EU

Security Advisory 2023-047

RCE Vulnerability in FortiOS and FortiProxy

July 13, 2023 — v1.0

TLP:CLEAR

History:

- *13/07/2023 — v1.0 – Initial publication*

Summary

On July 11, 2023, Fortinet released an advisory regarding a critical vulnerability in FortiOS & FortiProxy that may allow remote attackers to execute arbitrary code or command via crafted packets [1]. This vulnerability was identified as `CVE-2023-33308` with CVSS score of 9.8.

Due to the level of access and control on the network, we recommend to update as soon as possible.

Technical Details

This vulnerability is the result of a stack-based overflow vulnerability in FortiOS & FortiProxy. A remote attacker can send crafted packets reaching proxy policies or firewall policies with proxy mode alongside SSL deep packet inspection to execute arbitrary code or command.

Affected Products

- FortiOS version 7.2.0 through 7.2.3
- FortiOS version 7.0.0 through 7.0.10
- FortiProxy version 7.2.0 through 7.2.2
- FortiProxy version 7.0.0 through 7.0.9

Recommendations

CERT-EU strongly recommends upgrading affected FortiOS & FortiProxy products to the latest version.

Workaround

It is possible to disable HTTP/2 support on SSL inspection profiles used by proxy policies or firewall policies with proxy mode [1,2].

References

[1] https://www.fortiguard.com/psirt/FG-IR-23-183

[2] https://docs.fortinet.com/document/fortigate/7.0.0/new-features/710924/http-2-support-in-proxy-mode-ssl-inspection