10 years CERT-EU

Security Advisory 2023-038

Critical Vulnerability in FortiOS

June 12, 2023 — v1.0

TLP:CLEAR

History:

- *12/06/2023 — v1.0 – Initial publication*

Summary

Fortinet has released several versions of FortiOS to patch a critical pre-authentication remote code execution (RCE) vulnerability in its Fortigate SSL VPN devices. The vulnerability, identified as CVE-2023-27997, allows a hostile agent to interfere via the VPN, even if Multi-Factor Authentication (MFA) is activated [1, 2].

Technical Details

The vulnerability, CVE-2023-27997, does not require the attacker to be logged in to exploit it and is reachable pre-authentication on every SSL VPN appliance. The exact nature of the vulnerability is currently not publicly announced, but it is expected that Fortinet will be releasing more details on June 13, 2023. This security advisory will be updated accordingly.

Affected Products

All previous versions of Fortinet's Fortigate firewalls and other devices are suspected to be affected by this vulnerability.

Recommendations

Given the severity of the vulnerability, enterprise administrators are advised to update their Fortigate devices as soon as possible. The vulnerability has been fixed in FortiOS firmware versions 6.0.17, 6.2.15, 6.4.13, 7.0.12, and 7.2.5.

References

[1] https://www.bleepingcomputer.com/news/security/fortinet-fixes-critical-rce-flaw-in-fortigate-ssl-vpn-devices-patch-now/

[2] https://www.helpnetsecurity.com/2023/06/11/cve-2023-27997/