Security Advisory 2023-038

Critical Vulnerability in FortiOS

June 13, 2023 — v1.1

TLP:CLEAR

History:

- *12/06/2023 — v1.0 – Initial publication*
- *13/06/2023 — v1.1 – Updated with information provided by Fortinet*

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 vulnerability is a heap-based overflow and may allow a remote attacker to execute arbitrary code via specifically crafted requests. While no public proof of concept is available at the writing of this security advisory, Fortinet notes that this vulnerability may have been exploited in a limited number of cases.
A number of additional vulnerabilities were also addressed in the patch.

Incident ID	NVD CVE	Product	CSSV	Description
FG-IR-23-111	CVE-2023-29180	FortiOS	7.3	Null pointer de-reference in SSLVPNd
FG-IR-22-475	CVE-2023-22640	FortiOS	7.1	Out-of-bound-write in SSLVPNd
FG-IR-23-119	CVE-2023-29181	FortiOS	8.3	Format String Bug in Fclicense daemon
FG-IR-23-125	CVE-2023-29179	FortiOS	6.4	Null pointer de-reference in SSLVPNd proxy
FG-IR-22-479	CVE-2023-22641	FortiOS	4.1	Open redirect in SSLVPNd

Affected Products

At least the following FortiOS-6K7K versions are impacted:

- FortiOS-6K7K version 7.0.10
- FortiOS-6K7K version 7.0.5
- FortiOS-6K7K version 6.4.12
- FortiOS-6K7K version 6.4.10
- FortiOS-6K7K version 6.4.8

- FortiOS-6K7K version 6.4.6
- FortiOS-6K7K version 6.4.2
- FortiOS-6K7K version 6.2.9 through 6.2.13
- FortiOS-6K7K version 6.2.6 through 6.2.7
- FortiOS-6K7K version 6.2.4
- FortiOS-6K7K version 6.0.12 through 6.0.16
- FortiOS-6K7K version 6.0.10

At least the following FortiProxy versions are impacted:

- FortiProxy version 7.2.0 through 7.2.3
- FortiProxy version 7.0.0 through 7.0.9
- FortiProxy version 2.0.0 through 2.0.12
- FortiProxy 1.2 all versions
- FortiProxy 1.1 all versions

At least the following FortiOS versions are impacted:

- FortiOS version 7.2.0 through 7.2.4
- FortiOS version 7.0.0 through 7.0.11
- FortiOS version 6.4.0 through 6.4.12
- FortiOS version 6.0.0 through 6.0.16

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 the following versions:

- FortiOS-6K7K version 7.0.12 or above
- FortiOS-6K7K version 6.4.13 or above
- FortiOS-6K7K version 6.2.15 or above
- FortiOS-6K7K version 6.0.17 or above
- FortiProxy version 7.2.4 or above
- FortiProxy version 7.0.10 or above
- FortiProxy version 2.0.13 or above
- FortiOS version 7.4.0 or above
- FortiOS version 7.2.5 or above
- FortiOS version 7.0.12 or above
- FortiOS version 6.4.13 or above
- FortiOS version 6.2.14 or above
- FortiOS version 6.0.17 or above

In addition of updating, the vendor recommends the following actions [3]:

- review the systems for evidence of exploit of previous vulnerabilities, notably CVE-2022-04-0684 [4],
- follow hardening recommendations [5],
- minimise the attack surface by disabling unused features and managing devices via an out-of-band method wherever possible.

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/

[3] https://www.fortiguard.com/psirt/FG-IR-23-097

[4] https://www.fortiguard.com/psirt/FG-IR-22-377

[5] https://docs.fortinet.com/document/fortigate/7.2.0/best-practices/555436/hardening