Security Advisory 2023-015

RCE Vulnerability in Fortinet Products

March 8, 2023 — v1.0

TLP:CLEAR

History:

- *08/03/2023 — v1.0 – Initial publication*

Summary

On March 7, 2023, Fortinet released an advisory regarding one critical vulnerability in FortiOS and FortiProxy administrative interface. This vulnerability is identified as `CVE-2023-25610` (CVSS score of 9.3) and it may allow remote unauthenticated attackers to execute arbitrary code on the device and/or to perform a DoS on the GUI [1].

Fortinet is not aware of any instance where this vulnerability was exploited in the wild.

Technical Details

The vulnerability `CVE-2023-25610` is caused by a heap buffer underflow in the administrative interface, and may allow an unauthenticated attacker to execute arbitrary code on the device and/or to perform a DoS on the GUI, via specifically crafted requests.

Affected Products

The following devices/software versions are vulnerable to both arbitrary code execution, and DoS:

- FortiOS version 7.2.0 through 7.2.3
- FortiOS version 7.0.0 through 7.0.9
- FortiOS version 6.4.0 through 6.4.11
- FortiOS version 6.2.0 through 6.2.12
- FortiOS 6.0 all versions
- FortiProxy version 7.2.0 through 7.2.2
- FortiProxy version 7.0.0 through 7.0.8
- FortiProxy version 2.0.0 through 2.0.11
- FortiProxy 1.2 all versions
- FortiProxy 1.1 all versions

There are additional devices/software versions listed in the advisory [1] that are *only* impacted by the DoS part of the issue, *not* by the arbitrary code execution. Please check the extended list.

Recommendations

Upgrade FortiOS & FortiProxy products to:

- FortiOS version 7.4.0 or above
- FortiOS version 7.2.4 or above
- FortiOS version 7.0.10 or above
- FortiOS version 6.4.12 or above
- FortiOS version 6.2.13 or above
- FortiProxy version 7.2.3 or above
- FortiProxy version 7.0.9 or above
- FortiProxy version 2.0.12 or above
- FortiOS-6K7K version 7.0.10 or above
- FortiOS-6K7K version 6.4.12 or above
- FortiOS-6K7K version 6.2.13 or above

Workarounds

A workaround is available for FortiOS [1]:

- Disable HTTP/HTTPS administrative interface or limit IP addresses that can reach the administrative interface;
- Create an Address Group, then create the Local in Policy to restrict access only to the predefined group on management interface.

When using a HA reserved management interface, the local-in policy needs to be configured slightly differently [2].

References

[1] https://www.fortiguard.com/psirt/FG-IR-23-001

[2] https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-a-local-in-policy-on-a-HA/ta-p/222005