Security Advisory 2024-036

Vulnerabilities in Fortinet products

April 11, 2024 — v1.0

TLP:CLEAR

History:

- *11/04/2024 — v1.0 – Initial publication*

Summary

On April 11, 2024, Fortinet released multiple advisories regarding high and critical vulnerabilities affecting FortiOS, FortiProxy, FortiClient Mac and FortiClient Linux [1].

It is recommended upgrading affected software as soon as possible.

Technical Details

The vulnerability **CVE-2023-45590** [2], with a CVSS score of 9.4, is due to an improper control of generation of code. It may allow an unauthenticated attacker to execute arbitrary code via tricking a FortiClientLinux user into visiting a malicious website.

The vulnerabilities **CVE-2023-45588** and **CVE-2024-31492** [3], with a CVSS score of 7.8, are due to an external control of file name or path vulnerability. It may allow a local attacker to execute arbitrary code or commands via writing a malicious configuration file in `/tmp` before starting the installation process.

The vulnerability **CVE-2023-41677** [4], with a CVSS score of 7.5, is due to an insufficiently protected credential. It may allow an attacker to obtain the administrator cookie in rare and specific conditions, via tricking the administrator into visiting a malicious attacker-controlled website through the SSL-VPN.

Affected Products

The following product versions are affected:

CVE-2023-45590:

- FortiClientLinux version 7.2.0;
- FortiClientLinux version 7.0.6 through 7.0.10;
- FortiClientLinux version 7.0.3 through 7.0.4.

CVE-2023-45588 and **CVE-2024-31492**:

- FortiClientMac version 7.2.0 through 7.2.3;
- FortiClientMac version 7.0.6 through 7.0.10.

CVE-2023-41677:

- FortiOS version 7.4.0 through 7.4.1;
- FortiOS version 7.2.0 through 7.2.6;
- FortiOS version 7.0.0 through 7.0.12;
- FortiOS version 6.4.0 through 6.4.14;
- FortiOS version 6.2.0 through 6.2.15;
- FortiOS 6.0 all versions;
- FortiProxy version 7.4.0 through 7.4.1;
- FortiProxy version 7.2.0 through 7.2.7;
- FortiProxy version 7.0.0 through 7.0.13;
- FortiProxy 2.0 all versions;
- FortiProxy 1.2 all versions;
- FortiProxy 1.1 all versions;
- FortiProxy 1.0 all versions.

Recommendations

CERT-EU strongly recommends updating affected software to the latest versions by following the instructions given by the vendor [2,3,4].

References

[1] https://www.securityweek.com/fortinet-patches-critical-rce-vulnerability-in-forticlientlinux/

[2] https://www.fortiguard.com/psirt/FG-IR-23-087

[3] https://www.fortiguard.com/psirt/FG-IR-23-345

[4] https://www.fortiguard.com/psirt/FG-IR-23-493