CERT-EU

Security Advisory 2023-012

RCE vulnerabilities in Fortinet products

February 20, 2023 — v1.0

TLP:CLEAR

History:

- *20/02/2023 — v1.0 – Initial publication*

Summary

On February 16, 2023, Fortinet released advisories regarding critical vulnerabilities in FortiNAC and FortiWeb products that may allow unauthenticated attackers to perform remote arbitrary code or command execution [1].

The first vulnerability identified as `CVE-2022-39952` (CVSS score of 9.8) and is related to the FortiNAC product. FortiNAC is Fortinet's network access control solution that enhances the Security Fabric. It also provides protection against IoT threats, extends control to third-party devices, and orchestrates automatic responses to a wide range of networking events [2,3]. The second vulnerability identified as `CVE-2021-42756` (CVSS score of 9.8) and is related to FortiWeb products. FortiWeb is a web application firewall (WAF) that protects web applications and APIs from attacks that target known and unknown exploits and helps maintain compliance with regulations [4,5].

Technical Details

The vulnerability `CVE-2022-39952` is due to an external control of file name or path vulnerability in FortiNAC web server, and may allow an unauthenticated attacker to perform arbitrary write on the system [6].

The vulnerability `CVE-2021-42756` is due to multiple stack-based buffer overflow vulnerabilities in FortiWeb's proxy daemon, and may allow an unauthenticated remote attacker to achieve arbitrary code execution via specifically crafted HTTP requests [7].

Affected Products

CVE-2022-39952 [6]:

- FortiNAC version 9.4.0;
- FortiNAC version 9.2.0 through 9.2.5;
- FortiNAC version 9.1.0 through 9.1.7;
- FortiNAC 8.8 all versions;
- FortiNAC 8.7 all versions;
- FortiNAC 8.6 all versions;
- FortiNAC 8.5 all versions;
- FortiNAC 8.3 all versions.

CVE-2021-42756 [7]:

- FortiWeb 5.x all versions;
- FortiWeb versions 6.0.7 and below;
- FortiWeb versions 6.1.2 and below;
- FortiWeb versions 6.2.6 and below;
- FortiWeb versions 6.3.16 and below;
- FortiWeb 6.4 all versions.

Recommendations

Upgrade FortiNAC products to [6]:

- FortiNAC version 9.4.1 or above;
- FortiNAC version 9.2.6 or above;
- FortiNAC version 9.1.8 or above;
- FortiNAC version 7.2.0 or above.

Upgrade FortiWeb products to [7]:

- FortiWeb 7.0.0 or above;
- FortiWeb 6.3.17 or above;
- FortiWeb 6.2.7 or above;
- FortiWeb 6.1.3 or above;
- FortiWeb 6.0.8 or above.

References

[1] https://www.bleepingcomputer.com/news/security/fortinet-fixes-critical-rce-flaws-in-fortinac-and-fortiweb/

[2] https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf

[3] https://nvd.nist.gov/vuln/detail/CVE-2022-39952

[4] https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiWeb.pdf

[5] https://nvd.nist.gov/vuln/detail/CVE-2021-42756

[6] https://www.fortiguard.com/psirt/FG-IR-22-300

[7] https://www.fortiguard.com/psirt/FG-IR-21-186