SECURING Maryland INFORMATION SHARING AND ANALYSIS CENTER MD

POWERED BY ANOMALI

THREAT BULLETIN

VAR20240209-001.1 [Vulnerability Advisory Report] Vulnerabilities Found In FortiOS Could Allow For Remote Code Execution And Other Attacks

TLP
Clear

DESCRIPTION

TLP:CLEAR = Disclosure is not limited.

Summary

The following is being reported by MS-ISAC:

> Multiple vulnerabilities have been discovered in FortiOS, the most severe of which could allow for remote code execution. FortiOS is Fortinet's operating system used across many Fortinet devices. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution in the context of the system. Depending on the privileges associated with the service account, an attacker could then install programs; view, change, or delete data. Service accounts that are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights. Fortinet reports that CVE-2024-21762 is potentially being exploited in the wild.

Mitigations

The MD-ISAC recommends that organizations that use Fortinet appliances running FortiOS versions 6.0, 6.2, 6.4, 7.0, 7.2, 7.4, and 7.6 and FortiProxy versions 7.0, 7.2, and 7.4 review the advisories below and ensure that their systems are upgraded to the latest patched versions.

CVE-2024-21762 Details

NVD Summary: A out-of-bounds write in Fortinet FortiOS versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, 6.4.0 through 6.4.14, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17, FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, 2.0.0 through 2.0.13, 1.2.0 through 1.2.13, 1.1.0 through 1.1.6, 1.0.0 through 1.0.7 allows attacker to execute unauthorized code or commands via specifically crafted requests
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-21762

CWE ID: 787
Advisories, Assessments, and Mitigations: https://fortiguard.com/psirt/FG-IR-24-015

CVE-2024-23113 Details

NVD Summary: Not yet disclosed.
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-21762

CWE ID: None
Advisories, Assessments, and Mitigations: https://www.fortiguard.com/psirt/FG-IR-24-029

CVE-2023-47537 Details

NVD Summary: Not yet disclosed.
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-47537

CWE ID: None
Advisories, Assessments, and Mitigations: https://www.fortiguard.com/psirt/FG-IR-23-301

CVE-2023-44487 Details

NVD Summary: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-44487

CWE ID 400
Advisories, Assessments, and Mitigations: https://www.fortiguard.com/psirt/FG-IR-23-397

Incident Response

If administrators discover signs of attack or system compromise, the MD-ISAC recommends they:

- Immediately isolate affected systems.
- Collect and review relevant logs, data, and artifacts.
- Consider soliciting support from a third-party incident response organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
- Report incidents to MD-ISAC via Maryland's 24/7 Operations Center (md-isac@maryland.gov or (410) 697-9700 - option #5).

Reporting and Contact Information

In the case of a cybersecurity incident related to information found in this threat bulletin, Md. Code, Public Safety Article § 14-104.1 (c)(2) and Md. Code, State Finance & Procurement Article § 3.5-406(b)(2)) mandate that you report this via the Maryland Incident Reporting System. It is also recommended that you submit any shareable cyber threat intelligence to the MD-ISAC via the MD-ISAC Threat Intelligence Platform (TIP).

TLP:CLEAR = Disclosure is not limited.

TLP:CLEAR = Disclosure is not limited. Sources may use **TLP:CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Recipients may share **TLP:CLEAR** information without restriction. Information is subject to standard copyright rules.
For more information about Traffic Light Protocol (TLP) definitions and usage: https://www.cisa.gov/tlp