Security Advisory 2024-018

Critical Vulnerabilities in FortiOS

February 9, 2024 — v1.0

TLP:CLEAR

History:

- *09/02/2024 — v1.0 – Initial publication*

Summary

On February 9, 2024, Fortinet released an advisory regarding critical vulnerabilities affecting FortiOS that, if exploited, would allow a remote and unauthenticated to execute code on the affected device.

One of the critical vulnerabilities is potentially being exploited in the wild. It is recommended updating as soon as possible.

Technical Details

The vulnerability **CVE-2024-21762** [1], with a CVSS score of 9.8, is due to incorrect parameter checks in FortiOS SSL-VPN. When exploited by a remote and unauthenticated attacker via crafted HTTP requests, a reduced number of bytes could be copied outside buffer bounds, leading to memory corruption and flow redirection. This allows execution of arbitrary code or command.

The vulnerability **CVE-2024-23113** [2], with a CVSS score of 9.8, is due to an externally controlled format string vulnerability in FortiOS fgfmd daemon, and may allow a remote unauthenticated attacker to execute arbitrary code or commands via specially crafted requests.

Affected Products

The following product versions are affected:

- FortiOS version 7.4.0 through 7.4.2;
- FortiOS version 7.2.0 through 7.2.6;
- FortiOS version 7.0.0 through 7.0.13;
- FortiOS version 6.4.0 through 6.4.14;
- FortiOS version 6.2.0 through 6.2.15;
- FortiOS 6.0 all versions (only affected by CVE-2024-21762).

Recommendations

CERT-EU recommends updating or upgrading to a non-vulnerable version of the product as soon as possible.

References

[1] https://www.fortiguard.com/psirt/FG-IR-24-015

[2] https://www.fortiguard.com/psirt/FG-IR-24-029