Security Advisory 2024-059

Vulnerability in FortiOS

June 17, 2024 — v1.0

TLP:CLEAR

History:

- *17/06/2024 — v1.0 – Initial publication*

Summary

On June 12, 2024, Fortinet disclosed a high-severity vulnerability identified as **CVE-2024-23110** affecting FortiOS. This vulnerability allows an authenticated attacker to execute unauthorised code or commands via specially crafted command line arguments. The issue arises from multiple stack-based buffer overflow security defects in the command line interpreter.

No proof of concept is currently available at the moment, nevertheless CERT-EU strongly recommends patching affected products as soon as possible.

Technical details

CVE-2024-23110, with a CVSS score of 7.4, impacts FortiOS versions 6.x and 7.x. Exploitation may enable an authenticated attacker to execute unauthorised code or commands through specially crafted command line arguments.

Affected Products

The following FortiOS versions are affected:

- 6.x before 6.2.16
- 6.x before 6.4.15
- 7.x before 7.0.14
- 7.x before 7.2.7
- 7.x before 7.4.3

Recommendations

It is strongly recommended to update to the following fixed versions:

- FortiOS 6.2.16
- FortiOS 6.4.15
- FortiOS 7.0.14
- FortiOS 7.2.7
- FortiOS 7.4.3

References

[1] https://www.fortiguard.com/psirt/FG-IR-23-460

[2] https://www.securityweek.com/fortinet-patches-code-execution-vulnerability-in-fortios/