Newscast
Critical vulnerabilities in Fortinet

Table of content

Fortinet

On 8 February 2024, Fortinet published 7 advisories concerning vulnerabilities in their products. The two most critical vulnerabilities, CVE-2024-21762 and CVE-2024-23113, affect FortiOS.

CVE-2024-21762

EPSS	Exploited Remote code execution	POC
Pending	9.8 CRITICAL	NO
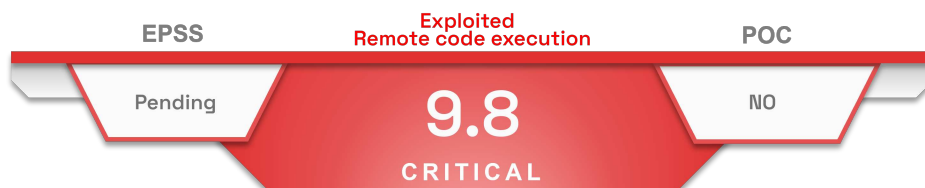
This vulnerability caused by a memory control flaw in FortiOS's *SSL-VPN*. It allows an unauthenticated attacker to execute arbitrary code via specially crafted requests.

🔥 | This vulnerability is exploited.

Type of vulnerability

- **CWE-787**: Out-of-bounds Write

Risk

- Remote code execution

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

FortiOS :

- Versions 6.0.x prior to 6.0.17 (included)
- Versions 6.2.x prior to 6.2.15 (included)
- Versions 6.4.x prior to 6.4.14 (included)
- Versions 7.0.x prior to 7.0.13 (included)
- Versions 7.2.x prior to 7.2.6 (included)
- Versions 7.4.x prior to 7.4.2 (included)

Recommendations

- Update FortiOS to version 6.2.16, 6.4.15, 7.0.14, 7.2.7, 7.4.3, 7.6 or later.
- If the Patch cannot be applied, Fortinet recommend deactivating the *SSL-VPN*.
- Additional information is available in Fortinet's advisory.

Proof of concept

To date, no proof of concept is available in open source.

CVE-2024-23113

EPSS	Remote code execution	POC
Pending	**9.8** **CRITICAL**	NO
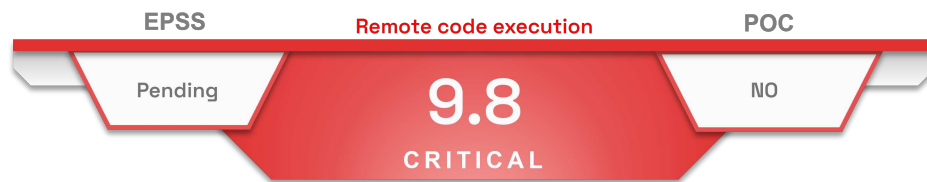
This flaw is due to a lack of control of data sent by the user in the *FortiGate to FortiManager Deamon* (*FGFMD*) of FortiOS. By sending crafted requests, an unauthenticated attacker can execute arbitrary code.

Type of vulnerability

- **CWE-134**: Use of Externally-Controlled Format String

Risk

- Remote code execution

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

FortiOS :

- Versions 7.0.x prior to 7.0.13 (included)
- Versions 7.2.x prior to 7.2.6 (included)
- Versions 7.4.x prior to 7.4.2 (included)

Recommendations

- Update FortiOS to version 7.0.14, 7.2.7, 7.4.3, 7.6 or later.
- Additional information is available in Fortinet's advisory.

Proof of concept

To date, no proof of concept is available in open source.

Sources

- https://www.cve.org/CVERecord?id=CVE-2024-21762
- https://www.cve.org/CVERecord?id=CVE-2024-23113
- https://www.fortiguard.com/psirt/FG-IR-24-015
- https://fortiguard.fortinet.com/psirt/FG-IR-24-029
- https://thehackernews.com/2024/02/fortinet-warns-of-critical-fortios-ssl.html