Security for the greater good

Newscast

Critical vulnerabilities in Fortinet

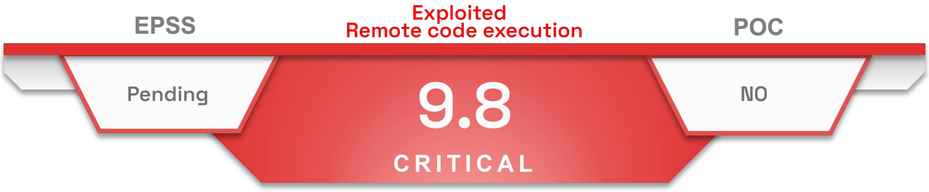
2024-02-15 I **TLP:CLEAR** I CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

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



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)

FortiProxy:

- All versions 1.0
- All versions 1.1
- All versions 1.2
- Versions 2.0.x prior to 2.0.13 (included)
- Versions 7.0.x prior to 7.0.14 (included)

- Versions 7.2.x prior to 7.2.8 (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 or later.
- Update FortiProxy to version 2.0.14, 7.0.15, 7.2.9, 7.4.3 or later.
- If the Patch cannot be applied, Fortinet recommend disabling 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

Pending

Remote code execution

9.8

CRITICAL

POC

NO

This flaw is due to a lack of control of data sent by the user in the *FortiGate to FortiManager Daemon* (*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)

Workaround

If the patch cannot be applied, Fortinet recommends removing *fgfm* access for each instance by changing:

```
config system interface
    edit "portX"
         set allowaccess ping https ssh fgfm
    next
end
```

to:

```
config system interface
    edit "portX"
         set allowaccess ping https ssh
    next
end
```

This change will prevent FortiManager from discovering FortiGate. Connections from FortiGate will still work.

If the fgfm feature is necessary, Fortinet recommend configuring a local-in policy to restrict access to specified IPs.

Recommendations

- Update FortiOS to version 7.0.14, 7.2.7, 7.4.3 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