Security Advisory 2024-028

Vulnerabilities in Fortinet Products

March 14, 2024 — v1.0

TLP:CLEAR

History:

- *14/03/2024 — v1.0 – Initial publication*

Summary

On March 12, 2024, Fortinet released fixes for three vulnerabilities affecting some of their products. The vulnerabilities could allow an unauthenticated attacker to execute unauthorised code or commands via specifically crafted requests.

It is recommended upgrading affected software as soon as possible.

Technical Details

The vulnerability `CVE-2023-48788` (CVSS score: 9.3) is an SQL injection in the DB2 Administration Server (DAS) component. It impacts FortiClient EMS versions 7.0 (7.0.1 through 7.0.10) and 7.2 (7.2.0 through 7.2.2), and it allows unauthenticated attackers to gain RCE with SYSTEM privileges on unpatched servers in low-complexity attacks that don't require user interaction [1].

The vulnerability `CVE-2023-42789` (CVSS score: 9.3) in the FortiOS and FortiProxy is a an out-of-bounds write vulnerability that could let an unauthenticated *inside attacker* (who has access to captive portal) remotely execute unauthorised code or commands on unpatched using maliciously crafted HTTP requests [2].

The vulnerability `CVE-2023-42790` (CVSS score: 9.3) in the FortiOS and FortiProxy is a stack-based buffer overflow that allows an unauthenticated *inside attacker* (who has access to captive portal) to execute arbitrary code or commands via specially crafted HTTP requests.

Affected Products

For the `CVE-2023-48788` :

- FortiClientEMS 7.2.0 through 7.2.2
- FortiClientEMS 7.0.1 through 7.0.10

For the `CVE-2023-42789` and `CVE-2023-42790` :

- FortiOS version 7.4.0 through 7.4.1
- FortiOS version 7.2.0 through 7.2.5
- FortiOS version 7.0.0 through 7.0.12

- FortiOS version 6.4.0 through 6.4.14
- FortiOS version 6.2.0 through 6.2.15
- FortiProxy version 7.4.0
- FortiProxy version 7.2.0 through 7.2.6
- FortiProxy version 7.0.0 through 7.0.12
- FortiProxy version 2.0.0 through 2.0.13

Recommendations

For the `CVE-2023-48788` :

- Upgrade to FortiClientEMS to 7.2.3 or ab ove
- Upgrade to FortiClientEMS to 7.0.11 or above

For the `CVE-2023-42789` and `CVE-2023-42790` :

- Upgrade to FortiOS version 7.4.2 or above
- Upgrade to FortiOS version 7.2.6 or above
- Upgrade to FortiOS version 7.0.13 or above
- Upgrade to FortiOS version 6.4.15 or above
- Upgrade to FortiOS version 6.2.16 or above
- Upgrade to FortiProxy version 7.4.1 or above
- Upgrade to FortiProxy version 7.2.7 or above
- Upgrade to FortiProxy version 7.0.13 or above
- Upgrade to FortiProxy version 2.0.14 or above

Workarounds

For the second and third vulnerability `CVE-2023-42789` and `CVE-2023-42790`, a workaround is possible by setting a non-form-based authentication scheme :

```
config authentication scheme
edit scheme
set method <method>
next
end
```

Where the variable could be any of those settings :

```
- ntlm NTLM authentication.
- basic Basic HTTP authentication.
- digest Digest HTTP authentication.
- negotiate Negotiate authentication.
- fsso Fortinet Single Sign-On (FSSO) authentication.
- rsso RADIUS Single Sign-On (RSSO) authentication.
- ssh-publickey Public key based SSH authentication.
- cert Client certificate authentication.
- saml SAML authentication
```

CERT-EU strongly recommends updating affected software to the latest versions by following the instructions given by the vendor [1].

References

[1] https://fortiguard.fortinet.com/psirt/FG-IR-24-007

[2] https://www.fortiguard.com/psirt/FG-IR-23-328