Security Advisory 2025-008

High Vulnerabilities in Fortinet Products

2025-03-14 — v1.0

TLP:CLEAR

History:

- *14/03/2025 — v1.0 – Initial publication*

Summary

On March 11, 2025, Fortinet released several security advisories addressing 18 vulnerabilities ranging from low to high severity [1].

It is recommended updating as soon as possible.

Technical Details

- The vulnerability **CVE-2023-48790**, with a CVSS score of 7.1, is a cross-site request forgery vulnerability in FortiNDR that may allow a remote unauthenticated attacker to execute unauthorised actions via crafted HTTP GET requests [2].
- The vulnerability **CVE-2024-45324**, with a CVSS score of 7.0, is a use of externally controlled format string vulnerability in FortiOS, FortiProxy, FortiPAM, FortiSRA and FortiWeb that may allow a privileged attacker to execute unauthorised code or commands via specially crafted HTTP or HTTPS commands [3].
- The vulnerability **CVE-2023-40723**, with a CVSS score of 7.7, is an exposure of sensitive information to an unauthorised actor in FortiSIEM that may allow a remote unauthenticated attacker who acquired knowledge of the agent's authorisation header by other means to read the database password via crafted api requests [4].

Fortinet also fixes low and medium severity vulnerabilities in their products [1].

Affected Products

The vulnerability **CVE-2023-48790** affects the following products and versions [2]:

- FortiNDR 7.4 version 7.4.0
- FortiNDR 7.2 versions 7.2.0 through 7.2.1
- FortiNDR 7.1 versions 7.1.0 through 7.1.1
- FortiNDR 7.0 versions 7.0.0 through 7.0.5
- FortiNDR 1.5 all versions

The vulnerability **CVE-2024-45324** affects the following products and versions [3]:

- FortiOS 7.4 versions 7.4.0 through 7.4.4
- FortiOS 7.2 versions 7.2.0 through 7.2.9
- FortiOS 7.0 versions 7.0.0 through 7.0.15
- FortiOS 6.4 versions 6.4.0 through 6.4.15
- FortiOS 6.2 all versions
- FortiPAM 1.4 versions 1.4.0 through 1.4.2
- FortiPAM 1.3 versions 1.3.0 through 1.3.1
- FortiPAM 1.2 all versions
- FortiPAM 1.1 all versions
- FortiPAM 1.0 all versions
- FortiProxy 7.6 version 7.6.0
- FortiProxy 7.4 versions 7.4.0 through 7.4.6
- FortiProxy 7.2 versions 7.2.0 through 7.2.12
- FortiProxy 7.0 versions 7.0.0 through 7.0.19
- FortiSRA 1.4 versions 1.4.0 through 1.4.2
- FortiWeb 7.6 version 7.6.0
- FortiWeb 7.4 versions 7.4.0 through 7.4.5
- FortiWeb 7.2 versions 7.2.0 through 7.2.10
- FortiWeb 7.0 versions 7.0.0 through 7.0.10

The vulnerability **CVE-2023-40723** affects the following products and versions [4]:

- FortiSIEM 6.7 versions 6.7.0 through 6.7.4
- FortiSIEM 6.6 versions 6.6.0 through 6.6.3
- FortiSIEM 6.5 versions 6.5.0 through 6.5.1
- FortiSIEM 6.4 versions 6.4.0 through 6.4.2
- FortiSIEM 6.3 all versions
- FortiSIEM 6.2 all versions
- FortiSIEM 6.1 all versions
- FortiSIEM 5.4 all versions
- FortiSIEM 5.3 all versions
- FortiSIEM 5.2 all versions
- FortiSIEM 5.1 all versions

Recommendations

CERT-EU recommends updating the affected products as soon as possible to the latest version.

References

[1] https://fortiguard.fortinet.com/psirt?page=1&date=2025&severity=&product=IPS%20Engine,FortiCloud,FortiWeb,FortiSIEMWindowsAgent,FortiSwitchManager,FortiWAN,FortiWLC,FortiAP-U,FortiSandbox,FSSO%20Windows%20DC%20Agent,FortiDeceptor,FortiAuthenticator,FortiRecorder,FortiTokenMobileWP,FortiTokenIOS,FortiSwitch,FortiFone,FortiAnalyzer%20Cloud,FortiClientAndroid,FortiNAC,FortiPresence,Meru%20AP,FortiTester,FortiNDR,FortiMail,FortiSIEM,FortiClientLinux,FortiAP-W2,FortiClientEMS,FortiClientWindows,FortiDDoS-CM,FortiExtender,FortiGuest,FortiManager%20Cloud,FortiDDoS-F,FortiPAM,FortiAnalyzer-BigData,FortiIsolator,FortiEDR%20Manager,FortiProxy,FortiClientMac,FSSO%20Windows%20CA,FortiConverter,FortiSOAR,FortiSASE,FortiLANCloud,FortiTokenAndroid,FortiNAC-F,FortiAnalyzer,FortiWebManager,FortiAP-C,FortiAP,FortiOS-6K7K,FortiOS,AV%20Engine,FortiAP-S,FortiVoice,FortiAIOps,FortiDDoS,FortiClientiOS,FortiManager,

FortiADC,FortiSDNConnector,FortiSRA,FortiADCManager,FortiEDR,FortiWLM,FortiPortal&component=&version=

[2] https://fortiguard.fortinet.com/psirt/FG-IR-23-353

[3] https://fortiguard.fortinet.com/psirt/FG-IR-24-325

[4] https://fortiguard.fortinet.com/psirt/FG-IR-23-117