CYBER ADVISORY

TLP:CLEAR

23 October 2024

Fortinet FortiManager Critical Flaw Exploited in Zero-Day Attacks

CVE-2024-47575 | Zero-Day | FortiManager | Fortinet

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a Fortinet FortiManager critical severity vulnerability known as CVE-2024-47575, with a CVSS score of 9.8.[1] This vulnerability may allow a remote, unauthenticated attacker to execute arbitrary code or commands via specially crafted requests, and has been exploited in the wild.[2] Successful exploitation of the FortiManager API vulnerability could allow attackers to execute commands, retrieve information, and take full control over managed devices to gain further access to corporate networks.[3]

This vulnerability affects multiple versions of FortiManager: [1]

- **FortiManager 7.6** (versions prior to 7.6.1)
- **FortiManager 7.4** (versions 7.4.0 through 7.4.4)
- **FortiManager 7.2** (versions 7.2.0 through 7.2.7)
- **FortiManager 7.0** (versions 7.0.0 through 7.0.12)
- **FortiManager 6.4** (versions 6.4.0 through 6.4.14)
- **FortiManager 6.2** (versions 6.2.0 through 6.2.12)

The Cal-CSIC recommends immediately updating the above versions of Fortimanager to their latest version.

For further information on applying updates or implementing workarounds, please refer to PSIRT | FortiGuard Labs. [2]

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Security Online; "Fortinet Warns of Actively Exploited Flaw in FortiManager: CVE-2024-47575 (CVSS 9.8)" https://securityonline.info/fortinet-warns-of-actively-exploited-flaw-in-fortimanager-cve-2024-47575-cvss-9-8/; Accessed 23OCT24
[2] Fortiguard Labs; "Missing Authentication in Fgfmsd" https://fortiguard.fortinet.com/psirt/FG-IR-24-423; Accessed 23OCT24
[3]Bleeping Computer; "Fortinet Warns of New Critical FortiManager Flaw Used in Zero-Day Attacks" https://www.bleepingcomputer.com/news/security/fortinet-warns-of-new-critical-fortimanager-flaw-used-in-zero-day-attacks/; Accessed 23OCT24