CYBER ADVISORY

TLP:CLEAR

12 March 2024

Multiple Fortinet Services Vulnerabilities

Fortinet | FortiOS | High Vulnerabilities | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of high and critical vulnerabilities, known as CVE-2023-47534, CVE-2023-42789, CVE-2023-42790, CVE-2024-23112, CVE-2023-36554 and CVE-2023-48788.[1] CVE-2023-47534 affects FortiClient EMS which may allow a remote and unauthenticated attacker to execute arbitrary commands on the admin workstation via creating malicious log entries with crafted requests to the server.[2] CVE-2023-42789 and CVE-2023-42790 affects FortiOS and FortiProxy captive portal which may allow an inside attacker who has access to captive portal to execute arbitrary code or commands via specially crafted HTTP requests.[3] CVE-2024-23112 affects FortiOS and FortiProxy SSLVPN which may allow an authenticated attacker to gain access to another user's bookmark via URL manipulation.[4] CVE-2023-36554 affects FortiWLM MEA for FortiManager which may allow an unauthenticated remote attacker to execute arbitrary code or commands via specifically crafted requests.[5] CVE-2023-48788 affects FortiClientEMS which may allow an unauthenticated attacker to execute unauthorized code or commands via specifically crafted requests.[6]

The Cal-CSIC recommends immediately applying the appropriated product upgrade.

For further information on applying upgrades, please refer to Fortinet Resources.

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] CISA; "Fortinet Releases Security Updates for Multiple Products;" https://www.cisa.gov/news-events/alerts/2024/03/12/fortinet-releases-security-updates-multiple-products; accessed 12 March 2024
[2] Fortiguard Labs; "FortiClientEMS - CSV injection in log download feature;" https://www.fortiguard.com/psirt/FG-IR-23-390; accessed 12 March 2024
[3] Fortiguard Labs; "FortiOS & FortiProxy - Out-of-bounds Write in captive portal;" https://www.fortiguard.com/psirt/FG-IR-23-328; accessed 12 March 2024
[4] Fortiguard Labs; "FortiOS & FortiProxy – Authorization bypass in SSLVPN bookmarks;" https://www.fortiguard.com/psirt/FG-IR-24-013; accessed 12 March 2024
[5] Fortiguard Labs; "FortiWLM MEA for FortiManager - improper access control in backup and restore features;" https://www.fortiguard.com/psirt/FG-IR-23-103; accessed 12 March 2024
[6] Fortiguard Labs; "Pervasive SQL injection in DAS component;" https://www.fortiguard.com/psirt/FG-IR-24-007; accessed 12 March 2024