



CYBER ADVISORY



CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

TLP: CLEAR

11 June 2024

FortiOS Vulnerability

CVE-2024-23110

FortiOS

Buffer Overflow

High Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a high vulnerability known as CVE-2024-23110.¹ The vulnerability lies in the command line interpreter of FortiOS.² The multiple stack-based buffer overflow vulnerability may allow an authenticated attacker to execute unauthorized code or commands via specially crafted command line arguments.³

Version	Affected
FortiOS 7.4	7.4.0 through 7.4.2
FortiOS 7.2	7.2.0 through 7.2.6
FortiOS 7.0	7.0.0 through 7.0.13
FortiOS 6.4	6.4.0 through 6.4.14
FortiOS 6.2	6.2.0 through 6.2.15
FortiOS 6.0	6.0 all versions

Table 1: Vulnerable FortiOS Products

The Cal-CSIC recommends upgrading to the appropriate fixed FortiOS version as soon as possible.

For further information on applying upgrades please refer to [Fortinet Upgrade Path Tool](#).

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

CAL-CSIC-202406-003

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP: CLEAR

CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

TLP:CLEAR

	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 FortiGuard Labs "Multiple buffer overflows in diag npu command;"

<https://www.fortiguards.com/psirt/FG-IR-23-460>; accessed 11 June 2024

² Vulners; "CVE-2024-23110;" <https://vulners.com/cvelist/CVELIST:CVE-2024-23110>; accessed 11 June 2024

³ Tenable; "CVE-2024-23110" <https://www.tenable.com/cve/CVE-2024-23110>; accessed 11 June 2024

CAL-CSIC-202406-003

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP:CLEAR