



CYBER ADVISORY

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

TLP:CLEAR

13 March 2024

Adobe ColdFusion Vulnerability

CVE-2024-20767

ColdFusion

RCE

Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-20767.¹ The vulnerability affects Adobe ColdFusion 2023 update 6 and earlier and ColdFusion 2021 update 12 and earlier across all platforms.² Exploitation of the vulnerability may allow an attacker to perform directory traversal attacks via remote code execution, (RCE).³

The Cal-CSIC recommends applying the appropriate ColdFusion upgrade as soon as possible.

For further information on applying upgrades, please refer to [Adobe Product Security Incident Response Team](#).

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

CAL-CSIC-202403-007

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

PUBLIC SERVICE ANNOUNCEMENT

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

TLP:CLEAR

	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 Cybersecurity Help; "#VU87392 Path traversal in ColdFusion;" <https://www.cybersecurity-help.cz/vulnerabilities/87392/>; accessed 13 March 2024

² Government of British Columbia; "Adobe VRM Team Alert;" https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/vulnerability-risk-management/vulnerability-reports/n24-101_adobe_security_advisory.pdf; accessed 13 March 2024

³ Adobe; "Security updates available for Adobe ColdFusion | APSB24-14;" <https://helpx.adobe.com/security/products/coldfusion/apsb24-14.html>; accessed 13 March 2024

CAL-CSIC-202403-006

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