CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

TLP:CLEAR
2 April 2025

CrushFTP Vulnerability

CrushFTP | Authentication Bypass | Multiple Versions | Actively Exploited

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability in the CrushFTP product known as CVE-2025-2825, with a CVSS v3.1 score of 9.8. This vulnerability affects multiple versions including, 10.0.0 through 10.8.3 and 11.0.0 through 11.3.0.[1] The vulnerability affects the S3 authorization header processing and allows an attacker to bypass authentication.[2] Attackers taking advantage of this vulnerability can conduct admin level actions and execute data retrieval remotely, with only a known username. Attackers are actively attempting to take advantage of this vulnerability utilizing the published proof of concept (POC) exploit code.[3]

The Cal-CSIC recommends immediately upgrading CrushFTP to the latest version.

For more information on updating to the latest version, please refer to the CrushFTP Wiki update page.

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.
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 Affairs; "CRUSHFTP CVE-2025-2825 FLAW ACTIVELY EXPLOITED IN THE WILD"; https://securityaffairs.com/176097/hacking/crushftp-cve-2025-2825-flaw-actively-exploited.html; accessed 2 April 2025.
[2] The Hacker News; "New Security Flaws Found in VMware Tools and CrushFTP – High Risk, PoC Released"; https://thehackernews.com/2025/03/new-security-flaws-found-in-vmware.html; accessed 2 April 2025.
[3] Project Discovery; "CrushFTP Authentication Bypass – CVE-2025-2825" https://projectdiscovery.io/blog/crushftp-authentication-bypass; accessed 2 April 2025.

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.