CYBER ADVISORY

TLP:CLEAR
23 April 2024

CrushFTP Zero Day Vulnerability

CVE-2024-4040 | Zero Day | CrushFTP | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of acritical vulnerability under active exploitation known as CVE-2024-4040.[1] The vulnerability affects CrushFTP in all versions before 10.7.1 and 11.1.0 on all platforms.[2] Exploitation may allow a remote attacker with low privileges to read files from the filesystem outside of VFS Sandbox.[3]

The Cal-CSIC recommends immediately upgrading to the appropriate patched version of CrushFTP.

For further information on applying patched versions of CrushFTP, please refer to CrushFTP Update.

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] Born's Tech and Windows World; "Update CrushFTP to v11.1.0, vulnerability (CVE-2024-4040) under attack;" https://borncity.com/win/2024/04/23/update-crushftp-to-v11-1-0-vulnerability-cve-2024-4040-under-attack/; accessed 23 April 2024

[2] Tenable; "CVE-2024-4040: CrushFTP Virtual File System (VFS) Sandbox Escape Vulnerability Exploited;" https://www.tenable.com/blog/cve-2024-4040-crushftp-virtual-file-system-vfs-sandbox-escape-vulnerability-exploited; accessed 23 April 2024

[3] Help Net Security; "CrushFTP zero-day exploited by attackers, upgrade immediately! (CVE-2024-4040);" https://www.helpnetsecurity.com/2024/04/23/cve-2024-4040/; accessed 23 April 2024