CYBER ADVISORY

TLP:CLEAR
03 October 2024

Zimbra Collaboration Vulnerability

CVE-2024-45519 | Zimbra | Active Exploitation | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability under active exploitation known as CVE-2024-45519, with a reported CVSS v3 rating of 10.0.[1] The OS command injection vulnerability affects Zimbra Collaboration before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1.[2] Exploitation of the vulnerability could allow an unauthenticated attacker to inject arbitrary commands via Remote Code Execution (RCE).[3]

The Cal-CSIC recommends immediately upgrading to the appropriate patched Zimbra Collaboration version.

For further information on applying upgrades please refer to Zimbra Security.

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] National Vulnerability Database; "CVE-2024-45519 Detail;" https://nvd.nist.gov/vuln/detail/CVE-2024-45519; accessed 03 October 2024
[2] HelpNet Security; "Critical Zimbra RCE vulnerability under mass exploitation (CVE-2024-45519)" https://www.helpnetsecurity.com/2024/10/02/cve-2024-45519-exploited/; accessed 03 October 2024
[3] SOC Radar; "RCE Vulnerability in Zimbra (CVE-2024-45519) Actively Exploited, Administrators Advised to Patch Immediately" https://socradar.io/rce-vulnerability-in-zimbra-cve-2024-45519/; accessed 03 October 2024