Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

TLP:CLEAR
12 January 2024

Gitlab Critical Vulnerabilities

CVE-2023-7028 | CVE-2023-5356 | CE/EE | Critical Vulnerability

Executive Summary

The California Cyber Threat Integration Center (Cal-CSIC) has become aware of vulnerabilities known as CVE-2023-7028 and CVE-2023-5356.[1] The vulnerabilities affect self-managed instances of GitLab Community Edition (CE) and Enterprise Edition (EE).[2] Exploitation of CVE-2023-7028 could allow attackers to facilitate account takeover by sending password reset emails to an unverified email address. Exploitation Of CVE-2023-5356 could allow a threat actor to abuse Slack/Mattermost integrations to execute slash commands as another user.[3,4]

The Cal-CSIC recommends immediately upgrading the affected instances to the appropriated patched version and to enable multi-factor authentication, (MFA).

For further information on applying patches, please refer to [GitLab Critical Security Release](#).

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.

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.

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 here.
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] Bleeping Computer; "GitLab warns of critical zero-click account hijacking vulnerability;" https://www.bleepingcomputer.com/news/security/gitlab-warns-of-critical-zero-click-account-hijacking-vulnerability/; accessed 12 January 2024

[2] Mitre; "CVE-2023-7028;" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-7028; accessed 12 January 2024

[3] The Hacker News; "Urgent: GitLab Releases Patch for Critical Vulnerabilities - Update ASAP;" https://thehackernews.com/2024/01/urgent-gitlab-releases-patch-for.html; accessed 12 January 2024

[4] SC Media; "GitLab vulnerability risks account takeover via simple password reset;" https://www.scmagazine.com/news/gitlab-vulnerability-risks-account-takeover-via-simple-password-reset; a2ccessed 12 January 2024

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.