Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

TLP:CLEAR
11 OCT 2024

GitLab Multiple Pipeline Vulnerabilities

GitLab | Pipeline | Community | Enterprise

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical rated vulnerability and multiple high rated vulnerabilities affecting Gitlab Community Edition (CE) and Gitlab Enterprise Edition (EE).[1] Exploitation of the most critical of these vulnerabilities allow unauthorized users to trigger Continuous Integration/Continuous Delivery (CI/CD) on automated processes, or pipelines, on any branch of the GitLab repository.[2] Bypassing these branch protections potentially allows an attacker to conduct code execution or gain access to sensitive information.[2]

Issue	CVE Identifier(s)	CVSS v3.1
Allows running pipelines in arbitrary branches in GitLab EE versions 12.5 prior to 17.2.9, starting from 17.3, prior to 17.3.5, and starting from 17.4 prior to 17.4.2	**CVE-2024-9164**	**9.6**
Allows an attacker to trigger a pipeline as another user under certain circumstances in GitLab CE/EE versions 11.6 prior to 17.2.9, starting from 17.3 prior to 17.3.5, and starting from 17.4 prior to 17.4.2	**CVE-2024-8970**	8.2
Instances with Product Analytics Dashboard configured and enabled could be vulnerable to SSRF attacks in GitLab EE versions 15.10 prior to 17.2.9, from 17.3 prior to 17.3.5, and from 17.4 prior to 17.4.2	**CVE-2024-8977**	**8.2**
Viewing diffs of MR with conflicts can be slow in GitLab CE/EE versions 13.6 prior to 17.2.9, starting from 17.3 prior to 17.3.5, and starting from 17.4 prior to 17.4.2	**CVE-2024-9631**	**7.5**
A cross-site scripting issue can be made to render as HTML under specific circumstances when authorizing a new application in GitLab versions 17.1 prior 17.2.9, starting from 17.3 prior to 17.3.5, and starting from 17.4 prior to 17.4.2	**CVE-2024-6530**	**7.3**

Table 1: Gitlab Multiple Pipeline Vulnerabilities [3]

The Cal-CSIC recommends immediately updating to Gitlab Community Edition and Enterprise Edition to versions 17.4.2, 17.9.5, and 17.2.9.

For further information on updating Gitlab Community Edition and Enterprise Edition please refer to GitLab Critical Patch Release: 17.4.2, 17.3.5, 17.2.9 | GitLab[3]

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 TLP:CLEAR rules, 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] The Hacker News; "New Critical GitLab Vulnerability Could Allow Arbitrary CI/CD Pipeline Execution" https://thehackernews.com/2024/10/new-critical-gitlab-vulnerability-could.html/; accessed 11 October 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.

[2] The Bleeping Computer; "GitLab warns of critical arbitrary branch pipeline execution flaw" https://www.bleepingcomputer.com/news/security/gitlab-warns-of-critical-arbitrary-branch-pipeline-execution-flaw/; accessed 09 October 2024

[3] GitLab; "GitLab Critical Patch Release: 17.4.2, 17.3.5, 17.2.9" https://about.gitlab.com/releases/2024/10/09/patch-release-gitlab-17-4-2-released/; accessed 11 October 2024