Vulnerability Advisory

TLP: CLEAR

CAL-CSIC-2026-10-A-014

14 OCT 2026

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

Unauthenticated Remote Code Execution Vulnerability Found within GitLab Community and Enterprise Edition

Integer Overflow Flaw	Remote Code Execution	Public Proof of Concept	Fixed Releases Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability in GitLab Community Edition (CE) and Enterprise Edition (EE). GitLab manages source code and automates Continuous Integration/Continuous Deliver/Deployment (CI/CD) workflows. CVE-2026-97229 is an integer overflow (CWE-190) in the CI/CD regular expression compiler, rated CVSS 3.1 10.0.[1]

Crafted regular expressions can enable unauthenticated code execution on the GitLab server. Open-source reporting demonstrates execution as the GitLab service account after malicious configuration and a specially named repository path are placed in a public project. Self-registration and public-project creation can enable this setup; the later trigger requires no authentication. A public proof of concept is available, but reporting reviewed on 14 October 2026 does not confirm exploitation in the wild.[2]

GitLab released patches on 12 October 2026, and urges affected self-managed installations to upgrade immediately. GitLab.com is already running the patched version, and GitLab Dedicated customers do not need to take action.[3]

The Cal-CSIC recommends clients running self-managed installations apply GitLab's updates immediately. Temporarily restrict anonymous public-project access and untrusted creation or modification of public projects. These controls reduce exposure to the demonstrated attack path but do not fix the vulnerability.

For additional details regarding CVE-2026-97229, please use this link:

GitLab Security Advisory:

https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/

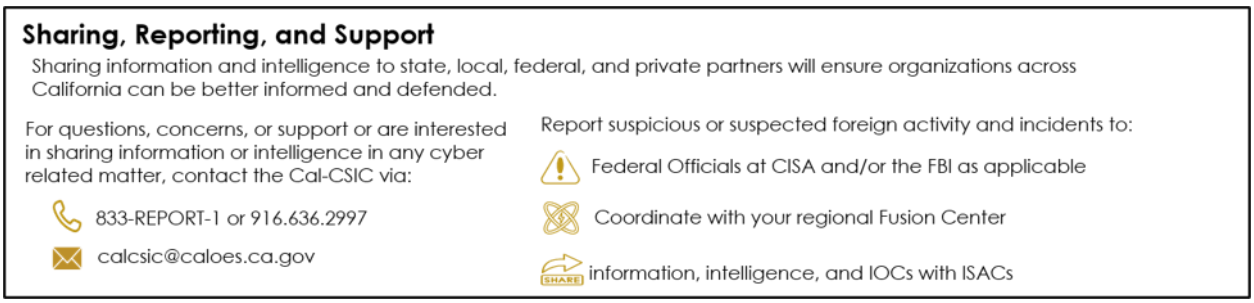
WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Affected Products and Versions

Product	Affected Version	Fixed Release
GitLab CE / EE	19.2.0 through 19.2.7	19.2.8
GitLab CE / EE	19.3.0 through 19.3.4	19.3.5
GitLab CE / EE	19.4.0 through 19.4.1	19.4.2

Note: The affected ranges apply to both GitLab CE and EE across deployment types. Upgrade to the fixed release for the installed branch or a later supported release containing the fix.[3]

Sharing, Reporting, and Support



References

[1] CVE Program (GitLab CNA); "CVE-2026-97229"; https://raw.githubusercontent.com/CVEProject/cvelistV5/main/cves/2026/97xxx/CVE-2026-97229.json; accessed 14 October 2026
[2] Rapid7; "CVE-2026-97229: Critical Unauthenticated Remote Code Execution in GitLab"; https://www.rapid7.com/blog/post/etr-cve-2026-97229-critical-unauthenticated-remote-code-execution-in-gitlab/; accessed 14 October 2026
[3] GitLab; "GitLab Critical Patch Release: 19.4.2, 19.3.5, 19.2.8"; https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/; accessed 14 October 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.