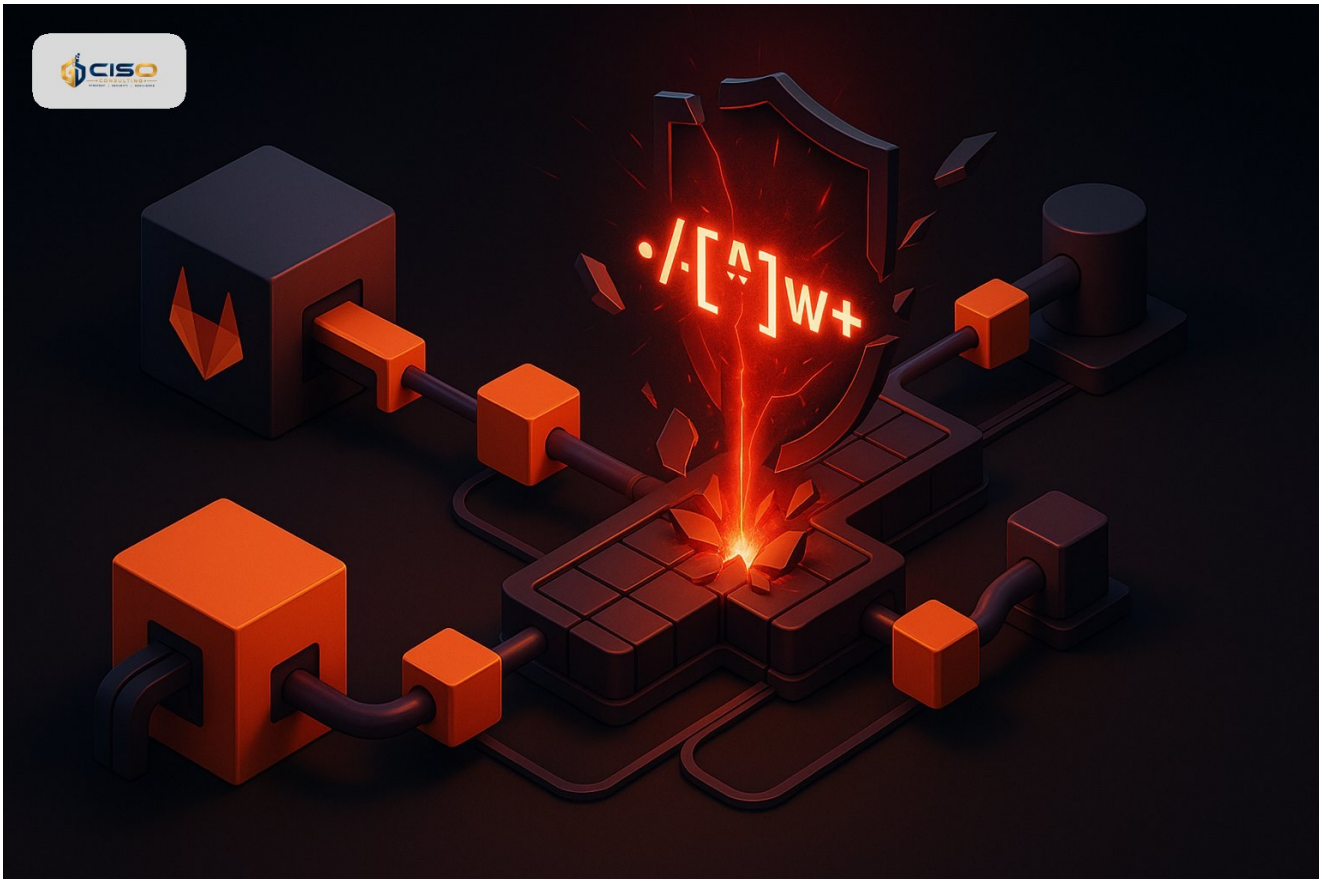


GitLab patches maximum-severity remote code execution flaw in CI/CD regex compiler



GitLab has released patches for a critical vulnerability allowing unauthenticated remote code execution through malicious regular expressions in CI/CD configuration files.

- CVE-2026-97229 is a maximum-severity integer overflow flaw in GitLab's CI/CD Regular Expression Compiler enabling remote code execution
- Unauthenticated attackers can exploit the vulnerability using specially crafted regular expressions in pipeline configuration files
- Patches released for GitLab CE and EE versions 19.2.8, 19.3.4, and 19.4.2; GitLab.com already patched
- The flaw was reported through GitLab's HackerOne bug bounty program by researcher 'joaxcar'
- GitLab has addressed multiple maximum-severity vulnerabilities in recent months, with CISA

Vulnerability details

GitLab has issued urgent security updates addressing **CVE-2026-97229**, a maximum-severity vulnerability in its CI/CD Regular Expression Compiler. The flaw stems from an integer overflow weakness that allows unauthenticated remote attackers to execute arbitrary code on vulnerable GitLab instances. The vulnerability affects the component responsible for parsing, compiling, and evaluating regular expressions in projects' pipeline configuration files.

According to GitLab's advisory, the issue could allow attackers to run code on GitLab servers through specially crafted regular expressions in CI/CD configurations due to insufficient validation. The vulnerability was discovered by a security researcher using the handle 'joaxcar' and reported through GitLab's HackerOne bug bounty program.

Affected versions and remediation

The security flaw impacts GitLab Community Edition and Enterprise Edition versions from 19.2 before 19.2.8, 19.3 before 19.3.4, and 19.4 before 19.4.2. GitLab has released patches for all affected versions and strongly recommends immediate upgrades for all self-managed installations. The company confirmed that GitLab.com is already running the patched version, while GitLab Dedicated customers do not need to take action.

Broader context

This vulnerability is the latest in a series of critical security issues affecting GitLab. In January, the platform patched a high-severity two-factor authentication bypass (CVE-2026-0723), and last month addressed another maximum-severity flaw (CVE-2026-85706) allowing unauthenticated data theft. The U.S. Cybersecurity and Infrastructure Security Agency added CVE-2026-85706 to its catalog of exploited vulnerabilities one day after disclosure, ordering federal agencies to patch within three days. CISA has catalogued five GitLab vulnerabilities exploited in attacks since November 2021, including one used by ransomware groups.

GitLab reports over 30 million registered users and adoption by more than half of Fortune 100 companies.

What to do now

1. Identify all self-managed GitLab Community Edition and Enterprise Edition instances within your organization's infrastructure
2. Immediately upgrade affected GitLab instances to patched versions 19.2.8, 19.3.4, or 19.4.2 depending on your current version branch
3. Review GitLab access logs for suspicious CI/CD pipeline configurations or unusual regular expression patterns submitted before patching

4. Verify that GitLab instances are not directly exposed to the internet without additional security controls such as VPN or IP whitelisting
5. Document the patching activity and timeline for compliance records under NCA ECC or SAMA CSF requirements
6. Brief development and DevOps teams on the vulnerability to ensure awareness of secure CI/CD configuration practices