An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2608250237

NCSC Advisory

Critical Vulnerability in GitLab CE/EE

CVE-2026-19478

25th, August 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-19478

Published: 2026-08-17

Vendor: GitLab

Product: GitLab

CVSS Score[1]: 9.4

Products Affected

Product	Version
GitLab	18.2 < 18.11.11
GitLab	19.0 < 19.0.8
GitLab	19.1 < 19.1.6
GitLab	19.2 < 19.2.4

Impact

GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.2 before 18.11.11, 19.0 before 19.0.8, 19.1 before 19.1.6, and 19.2 before 19.2.4 that under certain conditions could allow an unauthenticated user to remotely modify or delete public projects and user data via a GraphQL directive.

Common Weakness Enumeration (CWE)[2]: CWE-94: Improper Control of Generation of Code ('Code Injection')

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from GitLab.

- https://nvd.nist.gov/vuln/detail/CVE-2026-19478
- https://www.cve.org/CVERecord?id=CVE-2026-19478
- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-2-4-released/