Security Advisory 2025-011

Critical Vulnerabilities in Gitlab

2025-03-14 — v1.0

TLP:CLEAR

History:

- *14/03/2025 — v1.0 – Initial publication*

Summary

On March 13, 2025, GitLab released security updates for Community Edition (CE) and Enterprise Edition (EE), addressing nine vulnerabilities, including two critical severity flaws in the `ruby-saml` library used for SAML Single Sign-On (SSO) authentication [1].

It is recommended updating affected assets as soon as possible.

Technical Details

The critical vulnerabilities **CVE-2025-25291** and **CVE-2025-25292** affect the `ruby-saml` library. If exploited, it could allow an attacker with access to a valid signed SAML document to impersonate another user within the same SAML IdP environment. This can result in unauthorised access to another user's account.

The vulnerability **CVE-2025-27407** is a high-severity remote code execution issue in the Ruby `graphql` library. If exploited, it allows an authenticated attacker to exploit the Direct Transfer feature (disabled by default) for remote code execution.

Affected Products

These vulnerabilities affect GitLab Community Edition (CE) and Enterprise Edition (EE) versions prior to 17.7.7, 17.8.5, and 17.9.2.

Recommendations

CERT-EU recommends upgrading affected servers as soon as possible, prioritising Internet facing assets.

Workarounds

If immediate remediation is not possible, consider the following temporary mitigation:

- Ensure all users have two-factor authentication (2FA) enabled.
- Disable the `SAML two-factor bypass` option.

- Request admin approval for auto-created users by setting:

```
gitlab_rails['omniauth_block_auto_created_users'] = true
```

References

[1] https://about.gitlab.com/releases/2025/03/12/patch-release-gitlab-17-9-2-released/