Security Advisory 2022-041

Critical Vulnerability in GitLab

June 3, 2022 — v1.0

TLP:WHITE

History:

• 03/06/2022 — v1.0 – Initial publication

Summary

On June 1, 2022, GitLab released updates fixing several vulnerabilities, one of which could lead to Account Take Over [1]. This critical vulnerability is identified CVE-2022-1680 with a severity score of 9.9 out of 10.

Technical Details

When group SAML SSO is configured, the System for Cross-domain Management (SCIM) feature may allow any owner of a Premium group to invite arbitrary users through their username and email, then change those users’ email addresses via SCIM to an attacker controlled email address and thus - in the absence of 2FA - take over those accounts. It is also possible for the attacker to change the display name and username of the targeted account [2].

Affected Products

The following versions of GitLab Enterprise Edition are affected [2]:

• all versions starting from 11.10 and before 14.9.5,
• all versions starting from 14.10 and before 14.10.4,
• all versions starting from 15.0 and before 15.0.1.

To be vulnerable, the servers must be configured with SAML SSO option enabled.

Please note that the Cloud version GitLab.com is already running the last version.

Recommendations

CERT-EU strongly recommends updating GitLab servers to the last version.

CERT-EU also recommends enforcing multi-factor authentication (MFA) for users.
References
