Security Advisory 2024-101

Critical SAML Authentication Bypass in Gitlab

2024-09-19 — v1.0

TLP:CLEAR

History:

- *19/09/2024 — v1.0 – Initial publication*

Summary

On September 17, 2024, GitLab issued a security advisory addressing a critical vulnerability identified in GitLab's SAML authentication implementation, potentially allowing attackers to bypass authentication. The vulnerability affects the Community Edition (CE) and the Enterprise Edition (EE) instances that utilise SAML for single sign-on (SSO) [1,2].

It is recommended updating affected servers as soon as possible, and searching for potential successful exploitation of the vulnerability in the logs.

Technical Details

The vulnerability **CVE-2024-45409**, with a CVSS score of 10, arises from improper validation of SAML assertions, particularly the `extern_uid`, which uniquely identifies users. When a malicious SAML response is crafted, GitLab fails to verify critical elements in the SAML assertion, thus allowing the attacker to impersonate a legitimate user on the affected server. This vulnerability is due to issues in the OmniAuth-SAML and Ruby-SAML libraries. It was fixed by upgrading OmniAuth-SAML to version 2.2.1 and Ruby-SAML to 1.17.0.

Affected Products

The vulnerability affects GitLab CE and EE versions **prior to 17.3.3, 17.2.7, 17.1.8, 17.0.8, and 16.11.10** which have configured SAML based authentication [1].

Recommendations

CERT-EU strongly recommends updating affected GitLab CE and EE instances to a fixed version. It is also strongly advised to enforce Multi-Factor Authentication (MFA) for all accounts and enable the "Do not allow SAML 2FA bypass" setting to prevent attackers from bypassing the MFA requirement [1].

Moreover, it is recommended searching for potential exploitation of the vulnerability in the logs especially for Internet facing instances.

Detection

It is possible to detect a successful exploitation of the vulnerability in the `application_json` log file. It requires to review the `extern_uid` field attributes for unusual values. It is also possible to validate the findings by reviewing the corresponding SAML response, in the `auth_json` log file, by searching for incorrect or missing information in the `attributes` section [1].

Gitlab Security Engineering provides two detection methods that could be adapted to detect users with more than one unique `extern_uid` over time, and SAML authentication events from a different IP address than other identity provider (IdP) events for the same user over time.

References

[1] https://about.gitlab.com/releases/2024/09/17/patch-release-gitlab-17-3-3-released/

[2] https://www.bleepingcomputer.com/news/security/gitlab-releases-fix-for-critical-saml-authentication-bypass-flaw/