aDvens

Security for the greater good

Newscast

Critical vulnerability in GitLab

2024-01-12 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

GitLab - CVE-2023-7028

On 11 January 2024, GitLab published an alert concerning critical vulnerabilities in its Community Edition (CE) and Enterprise Edition (EE). CVE-2023-7028, considered to be the most critical, allows an attacker, by sending a specifically forged request to the Rest API, to reset user passwords and log into their account.

Even though MFA prevents an attacker from being able to log into one's account, it does not stop them from changing the password.

Risks

- Authentication bypass

Criticality (CVSS v3.1 base score)

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	None

Proof of concept

A proof of concept is available in open source.

Affected products

GitLab CE et EE :

- Versions 16.1 prior to 16.1.5
- Versions 16.2 prior to 16.2.8
- Versions 16.3 prior to 16.3.6
- Versions 16.4 prior to 16.4.4
- Versions 16.5 prior to 16.5.6
- Versions 16.6 prior to 16.6.4
- Versions 16.7 prior to 16.7.2

Recommendations

Update GitLab to version 16.1.5, 16.2.8, 16.3.6, 16.4.4, 16.5.6, 16.6.4, 16.7.2 or later.

GitLab recommends checking log files for the following elements:

- In the *gitlab-rails/production_json.log* file, HTTP requests to the */users/password* path containing several email addresses.
- In the *gitlab-rails/audit_json.log* file, entries with meta.caller.id of *PasswordsController#create* and *target_details* consisting of a JSON array containing several email addresses.

Additional information is available in GitLab's advisory.

Sources

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-7028
- https://about.gitlab.com/releases/2024/01/11/critical-security-release-gitlab-16-7-2-released/