CERT-EU

Security Advisory 2022-024

# Critical Vulnerability in Gitlab

*April 4, 2022 — v1.0*

**TLP:WHITE**

*History:*

- *04/04/2022 — v1.0 – Initial publication*

## Summary

On 31/03/2022, GitLab released an advisory for a critical password security vulnerability in GitLab Community and Enterprise products tracked as CVE-2022-1162. Discovered by the internal team of Gitlab, this vulnerability allows remote attacker to taker over user accounts. GitLab is not aware of accounts compromised by exploiting this vulnerability.

Evaluated with a score of 9.1 out of 10, CERT-EU recommends to patch **as soon as possible** [1].

## Technical Details

A hardcoded password was set for accounts registered using an OmniAuth provider (e.g., OAuth, LDAP, SAML) in GitLab CE/EE versions 14.7 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allowing attackers to potentially take over accounts.

## Affected Products

- Versions 14.7 to 14.7.6
- Versions 14.8 to 14.8.4
- Versions 14.9 to 14.9.1

## Recommendations

If you're running the affected versions of GitLab Community Edition/Enterprise Edition, it is highly recommended to upgrade the software to a patched version.

| Affected version | Patched version |
|---|---|
| 14.7.0 to 14.7.6 | 14.7.7 |
| 14.8.0 to 14.8.4 | 14.8.5 |
| 14.9.0 to 14.9.1 | 14.9.2 |

Additionally, Gitlab developers created a script that can be used by self-managed instance ad-

mins to identify users potentially impacted by this vulnerability [2].

## References

[1] https://about.gitlab.com/releases/2022/03/31/critical-security-release-gitlab-14-9-2-released/

[2] https://about.gitlab.com/releases/2022/03/31/critical-security-release-gitlab-14-9-2-released/#script-to-identify-users-potentially-impacted-by-cve-2022-1162