CVE-2024-7102

EXECUTION WITH UNNECESSARY PRIVILEGE IN GITLAB

Vairav Advisory Report

Date: February 13, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Mobile: +977-9820105900

Thirbam Sadak 148

Baluwatar, Kathmandu

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A critical vulnerability (CVE-2024-7102) has been identified in GitLab CE/EE, affecting versions from 16.4 to 17.5.0. This vulnerability allows an attacker to trigger a pipeline as another user under specific conditions, potentially leading to unauthorized execution of code or privilege escalation.

VULNERABILITY DETAILS

CVE-2024-7102

Description: Execution with unnecessary privileges vulnerability in GitLab CE/EE allows an attacker to trigger a pipeline as another user under certain circumstances.

Impact: Unauthorized execution, privilege escalation.

CVSS Score: 9.6 (Critical).

AFFECTED VERSIONS

GitLab CE/EE:

- Affected: Versions from 16.4 before 17.5.0

EXPLOIT DETAILS

An attacker can exploit this vulnerability by executing pipelines on behalf of another user, potentially gaining unauthorized access or executing malicious code.

RECOMMENDED ACTIONS

- GitLab has released patches to mitigate this vulnerability. Users should upgrade to version 17.5.0 or later.

REFERENCES

https://app.opencve.io/cve/CVE-2024-7102

https://www.cve.org/CVERecord?id=CVE-2024-7102

https://nvd.nist.gov/vuln/detail/CVE-2024-7102

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com