Security Advisory 2022-048

Critical Remote Code Execution Vulnerability in GitLab

July 4, 2022 — v1.0

TLP:WHITE

History:

- *04/07/2022 — v1.0 – Initial publication*

Summary

On June 30, 2022, GitLab released new software versions that fix several vulnerabilities [1], one of which is a critical remote command execution vulnerability identified `CVE-2022-2185`, with a CVSS score of 9.9 out of 10 [2].

It is highly recommended to upgrade GitLab servers to the latest available version.

Technical Details

The vulnerability exists in the `Project Imports` feature where an **authorised** user could import a maliciously crafted project leading to remote code execution.

Affected Products

The following version of GitLab Community Edition (CE) and Enterprise Edition (EE) are affected:

- 14.0 prior to 14.10.5
- 15.0 prior to 15.0.4
- 15.1 prior to 15.1.1

Recommendations

CERT-EU strongly recommends upgrading all GitLab servers to the latest version as soon as possible.

References

[1] https://securityonline.info/cve-2022-2185-gitlab-remote-code-execution-vulnerability/

[2] https://about.gitlab.com/releases/2022/06/30/critical-security-release-gitlab-15-1-1-released/