Security Advisory 2022-062

Remote Command Execution Vulnerability in Gitlab

August 25, 2022 — v1.0

TLP:WHITE

History:

- *25/08/2022 — v1.0 – Initial publication*

Summary

On the 22nd of August 2022, GitLab released a security advisory regarding a Remote Command Execution affecting its products. This vulnerability exists in the `import via Github` functionality [1]. Exploiting this vulnerability, allows an authenticated user to achieve remote code execution on the affected server.

Details

The vulnerability is identified as `CVE-2022-2884` and has a severity score of 9.9 out of 10. [2] The issue is now mitigated in the latest release versions 15.3.1, 15.2.3, 15.1.5 for GitLab Community Edition (CE) and Enterprise Edition (EE).

Affected Products

- GitLab CE/EE - from 11.3.4 before 15.1.5
- GitLab CE/EE - from 15.2 before 15.2.3
- GitLab CE/EE - from 15.3 before 15.3.1

Workarounds

There is an available workaround to mitigate this vulnerability which consists in disabling GitHub import. Detailed information is available on the vendor's page. [1]

Recommendations

CERT-EU strongly recommends applying the latest updates as soon as possible.

References

[1] https://about.gitlab.com/releases/2022/08/22/critical-security-release-gitlab-15-3-1-released/

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2884