National Cyber Security Centre

2208261000-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Remote Command Execution via Github import - CVE-2022-2884 (CVSS 9.9)
26 August 2022

Status: TLP-WHITE

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-WHITE *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-WHITE *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

Gitlab have released details of a critical remote command execution vulnerability which affects GitLab Community Edition (CE) and Enterprise Edition (EE). This RCE vulnerability exists in all versions starting from 11.3.4 before 15.1.5, all versions starting from 15.2 before 15.2.3 and all versions starting from 15.3 before 15.3.1.

It allows an an authenticated user to achieve remote code execution via the Import from GitHub API endpoint.

Products Affected

All GitLab Community Edition and Enterprise Edition versions:

- Starting from 11.3.4 before 15.1.5
- Starting from 15.2 before 15.2.3
- Starting from 15.3 before 15.3.1

Impact

Remote Code Execution

Workarounds

If you are unable to upgrade right away, you can secure your GitLab installation against this vulnerability using the workaround outlined below until you have time to upgrade.

```
Disable GitHub import
```

Login using an administrator account to your GitLab installation and perform the following:

```
Click "Menu" -> "Admin".
Click "Settings" -> "General".
Expand the "Visibility and access controls" tab.
Under "Import sources" disable the "GitHub" option.
Click "Save changes"
```

Recommendations

The NCSC recommends that all installations running a version affected by the issues described above are upgraded to the latest version as soon as possible. More information can be found at: https://about.gitlab.com/releases/2022/08/22/critical-security-release-gitlab-15-3-1-released/

Updates can be found at the following link: https://about.gitlab.com/update/

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie