Security Advisory 2021-060

Critical Vulnerabilities in GitLab

November 3, 2021 — v1.0

TLP:WHITE

History:

- *03/11/2021 — v1.0 – Initial publication*

Summary

On April 14, 2021, GitLab published a security release to address CVE-2021-22205 [1], a critical remote code execution vulnerability in the service's web interface. In the meantime, it was proven that the vulnerability can be exploited unauthenticated. Moreover, recently it was announced that at least 50% of the 60,000 internet-facing GitLab installations are not patched against this critical RCE flaw [2].

Technical Details

CVE-2021-22205 [3] was initially assigned a CVSSv3 score of 9.9. However, on September 21, 2021 GitLab revised the CVSSv3 score to 10.0. The increase in score was the result of changing the vulnerability from requiring an authenticated user to an unauthenticated one.

Initially GitLab described the issue as an authenticated vulnerability that was the result of passing user-provided images to the service's embedded version of ExifTool. A remote attacker would execute arbitrary commands as the git user due to ExifTool's mishandling of DjVu files, an issue that was later assigned CVE-2021-22204. Unauthenticated and remote users are able to reach execution of ExifTool via GitLab by design. A curl command is sufficient to reach, and exploit, ExifTool [4].

Affected Products

This vulnerability affects versions 7.12 and later [1] except patched versions mentioned below.

Recommendations

Upgrade to patched versions:

- 13.10.3
- 13.9.6
- 13.8.8

CERT-EU recommends updating the vulnerable application as soon as possible.

Workarounds and Mitigations

To mitigate the vulnerability GitLab should not be exposed to Internet. If it still needs to be accessed remotely a VPN might be considered. For more details regarding Exposure and Mitigation Guidance please see [4].

References

[1] https://about.gitlab.com/releases/2021/04/14/security-release-gitlab-13-10-3-released/

[2] https://www.rapid7.com/blog/post/2021/11/01/gitlab-unauthenticated-remote-code-execution-cve-2021-22205-exploited-in-the-wild/

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22205

[4] https://attackerkb.com/topics/D41jRUXCiJ/cve-2021-22205/rapid7-analysis?referrer=blog