Hive Pro

THREAT ADVISORY

Thousands of GitLab instances impacted by multiple security flaws

TA2022046

Threat Level AMBER

Publish Date – March 4, 2022

Multiple security vulnerabilities have been discovered by researchers in GitLab, an open-source DevOps software. Some of these flaws could allow an unauthenticated remote attacker to retrieve all information linked to GitLab users and further launch brute force attacks.

The vulnerability tracked as CVE-2021-4191 is one of the prominent issue for which GitLab pushed a fix. This information disclosure vulnerability is caused by a missing authentication check when using the GitLab GraphQL API queries that may allow a remote, unauthenticated attacker to obtain registered GitLab usernames, names, and email addresses. Due to the availability of the Metasploit module, there is a probability that this vulnerability might be exploited in the wild.

Organizations should update to versions 14.8.2, 14.7.4, and 14.6.5 to remediate these vulnerabilities.

Potential MITRE ATT&CK TTPs are:
TA0001: Initial Access
T1190: Exploit-public facing application
TA0007: Discovery
T1087: Account Discovery
TA0006: Credential Access
T1110: Brute Force

Vulnerability Detail

CVE ID	Affected Version	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-4191	versions starting from 13.0, 14.4 to 14.7	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* , cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*	Unauthenticated user enumeration on GraphQL API	CWE-359
CVE-2022-0735	Versions 12.10 to 14.6.4, 14.7 to 14.7.3, 14.8 to 14.8.1	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* , cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*	Runner registration token disclosure through Quick Actions	CWE-200
CVE-2022-0549	All versions before 14.3.6, 14.4 to 14.4.3, 14.5 to 14.5.1	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* , cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*	Unprivileged users can add other users to groups through an API endpoint	CWE-284
CVE-2022-0751	All versions	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* , cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*	Inaccurate display of Snippet contents can be potentially misleading to users	CWE-284

Hive Pro

THREAT ADVISORY

CVE ID	Affected Version	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0741	All versions	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* , cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*	Environment variables can be leaked via the sendmail delivery method	CWE-200
CVE-2022-0738	Versions 14.6 to 14.6.4, 14.7 to 14.7.3, 14.8 to 14.8.1	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* , cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*	Adding a mirror with SSH credentials can leak password	CWE-200
CVE-2022-0489	All versions starting with 8.15	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* , cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*	Denial of Service via user comments	CWE-20

Patch Link

https://gitlab.com/gitlab-org/omnibus-gitlab/-/tree/14.8.2-Security-Hotpatches/config/patches/gitlab-rails
https://about.gitlab.com/update/
https://docs.gitlab.com/runner/install/linux-repository.html#updating-the-runner

References

https://about.gitlab.com/releases/2022/02/25/critical-security-release-gitlab-14-8-2-released/
https://github.com/rapid7/metasploit-framework/pull/16252
https://www.rapid7.com/blog/post/2022/03/03/cve-2021-4191-gitlab-graphql-api-user-enumeration-fixed/