Hive Pro

Threat Level

Green

THREAT ADVISORY

VULNERABILITY REPORT

Gitlab addresses critical security vulnerabilities with newer versions

Date of Publication	Admiralty code	TA Number
6 June 2022	A1	TA2022113

Summary

The new versions of Gitlab address one critical and two high security flaws (as per Gitlab). Some of these vulnerabilities could be exploited by an attacker to perform a Stored Cross-Site Scripting(XSS) attack. Organizations are encouraged to the update their installations to the latest version.

CVEs

CVE	NAME	PATCH
CVE-2022-1680	Account take over via SCIM email change	✓
CVE-2022-1940	Stored XSS in Jira integration	✓
CVE-2022-1948	Quick action commands susceptible to XSS	✓

Technical Details

#1

The first vulnerability CVE-2022-1680 exists in the SCIM feature which allows any premium owner to invite arbitrary users and change the SCIM to an attacker-controlled email, which could be exploited resulting in account takeover. The second vulnerability CVE-2022-1948 exists due to missing validation in quick actions which would allow an attacker to perform a Cross-Site Scripting(XSS) attack, by injecting HTML in contact details.

#2

The last vulnerability CVE-2022-1936 is a Stored Cross-Site Scripting(XSS), which would allow an attacker to execute arbitrary code on the victim's behalf via crafted Jira issues. Organizations must update their Gitlab instance to versions 15.0.1, 14.10.4, and 14.9.5 to remediate these vulnerabilities.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-1680	GitLab Enterprise Edition: 11.10.0 - 15.0.0	cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* , cpe:2.3:a:gitlab:gitlab:*:* :*:*:enterprise:*:*:*	CWE-284
CVE-2022-1940	GitLab Enterprise Edition: 13.11.0 - 15.0.0		CWE-79
CVE-2022-1948	Gitlab Community Edition: 15.0.0 GitLab Enterprise Edition: 15.0.0		

Patch Links

https://about.gitlab.com/update/

References

https://about.gitlab.com/releases/2022/06/01/critical-security-release-gitlab-15-0-1-released/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

6 June 2022 • 3:00 PM

More at www.hivepro.com