

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## GitLab Fixes Critical Account Takeover Vulnerability

Date of Publication

January 18, 2024

Last updated date

May 24, 2024

Admiralty Code

A1

TA Number

TA2024022





# Summary

**First Seen:** May 1, 2023

**Affected Platform:** GitLab Community Edition (CE) and Enterprise Edition (EE)

**Impact:** Critical GitLab vulnerability (CVE-2023-7028) enables unauthorized users to take over the administrator account without user interaction. Exploiting password reset flaws, attackers can submit two emails, both target as well as attacker account leading to complete account takeover. Users with two-factor authentication are safe, and GitLab urges immediate updates for affected versions to mitigate the issue in email verification.

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-7028	GitLab Account Takeover via Password Reset Vulnerability	GitLab CE/EE			
CVE-2023-4812	GitLab Merge Request Access Vulnerability	GitLab CE/EE			
CVE-2023-5356	GitLab Improper Authorization Vulnerability	GitLab CE/EE			
CVE-2023-6955	GitLab Improper Access Control Vulnerability	GitLab CE/EE			
CVE-2023-2030	GitLab Insufficient Verification of Data Authenticity Vulnerability	GitLab CE/EE			

# Vulnerability Details

## #1

GitLab has released patches for critical vulnerabilities in both its Community and Enterprise Editions. The most severe issue (CVE-2023-7028) allows account hijacking without user interaction, involving an authentication problem that permits password reset requests to be sent to arbitrary, unverified email addresses.

## #2

Even with two-factor authentication (2FA) active, a password reset is possible, but the second authentication factor is still needed for successful login. This vulnerability could have a significant impact on organizations using GitLab for hosting proprietary code and sensitive data.

## #3

Another high severity vulnerability CVE-2023-5356 enables attackers to abuse Slack/Mattermost integrations to execute slash commands as another user. Other fixed flaws include a high-severity vulnerability (CVE-2023-4812) allowing the bypassing of CODEOWNERS approval, improper access control (CVE-2023-6955) for Workspaces, and a commit signature validation flaw (CVE-2023-2030) impacting GitLab CE/EE versions 12.2 and onwards.

## #4

Immediate updates for all vulnerable versions, especially for self-hosted installations, are strongly recommended to mitigate potential risks. While there is no evidence of active exploitation of CVE-2023-7028, defenders should [check logs](#) for any signs of compromise.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-7028	Gitlab CE and EE versions 16.1 - 16.1.5, 16.2 - 16.2.8, 16.3 - 16.3.6, 16.4 - 16.4.4, 16.5 - 16.5.5, 16.6 - 16.6.3, 16.7 - 16.7.1	cpe:2.3:a:gitlab:gitlab_community_edition:*:*:*:*:*:* cpe:2.3:a:gitlab:gitlab_enterprise_edition:*:*:*:*:*:*	CWE-284
CVE-2023-4812	Gitlab CE and EE versions 15.3 - 16.5.4, 16.6 - 16.6.3, and 16.7 - 16.7.1	cpe:2.3:a:gitlab:gitlab_community_edition:*:*:*:*:*:* cpe:2.3:a:gitlab:gitlab_enterprise_edition:*:*:*:*:*:*	CWE-284

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-5356	Gitlab CE and EE versions 8.13 - 16.5.5, 16.6 - 16.6.3, 16.7 - 16.7.1	cpe:2.3:a:gitlab:gitlab_community_edition:*:*:*:*:*:* cpe:2.3:a:gitlab:gitlab_enterprise_edition:*:*:*:*:*:*	CWE-863
CVE-2023-6955	Gitlab CE and EE all versions prior to 16.5.6, 16.6 - 16.6.3 and 16.7 - 16.7.1	cpe:2.3:a:gitlab:gitlab_community_edition:*:*:*:*:*:* cpe:2.3:a:gitlab:gitlab_enterprise_edition:*:*:*:*:*:*	CWE-284
CVE-2023-2030	Gitlab CE and EE versions 12.2 - 16.5.5, 16.6 - 16.6.3, and 16.7 - 16.7.1	cpe:2.3:a:gitlab:gitlab_community_edition:*:*:*:*:*:* cpe:2.3:a:gitlab:gitlab_enterprise_edition:*:*:*:*:*:*	CWE-345

# Recommendations



**Apply Security Updates:** Promptly apply the latest patches provided by GitLab to address the specific vulnerabilities. Ensure that all instances of GitLab, including both Community and Enterprise Editions, are updated to the patched versions.



**Update GitLab Instances:** For self-hosted installations, manually update GitLab instances to the patched versions mentioned in the security advisories.



**Regularly Monitor Logs:** Monitor logs, particularly gitlab-rails/production\_json.log and gitlab-rails/audit\_json.log, for any suspicious activities or unauthorized access attempts related to password resets and slash command executions.



**Implement Strong Authentication Measures:** Enforce strong and secure authentication practices, such as enabling two-factor authentication (2FA) for all user accounts to add an additional layer of security.



**Review and Adjust Permissions:** Regularly review and adjust user permissions within GitLab to ensure that users have the minimum necessary access required for their roles, reducing the risk of unauthorized actions.

## Potential MITRE ATT&CK TTPs

<b><u>TA0001</u></b> Initial Access	<b><u>TA0002</u></b> Execution	<b><u>TA0042</u></b> Resource Development	<b><u>TA0005</u></b> Defense Evasion
<b><u>T1566</u></b> Phishing	<b><u>T1211</u></b> Exploitation for Defense Evasion	<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1203</u></b> Exploitation for Client Execution
<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.005</u></b> Exploits	<b><u>T1588.006</u></b> Vulnerabilities	

## Patch Links

Update GitLab versions to 16.5.6, 16.6.4, and 16.7.2.  
Critical vulnerability CVE-2023-7028 fix is also backported to versions 16.1.6, 16.2.9, 16.3.7, and 16.4.5.

Links:

<https://about.gitlab.com/releases/2024/01/11/critical-security-release-gitlab-16-7-2-released/>

<https://docs.gitlab.com/ee/update/#upgrade-paths>

## References

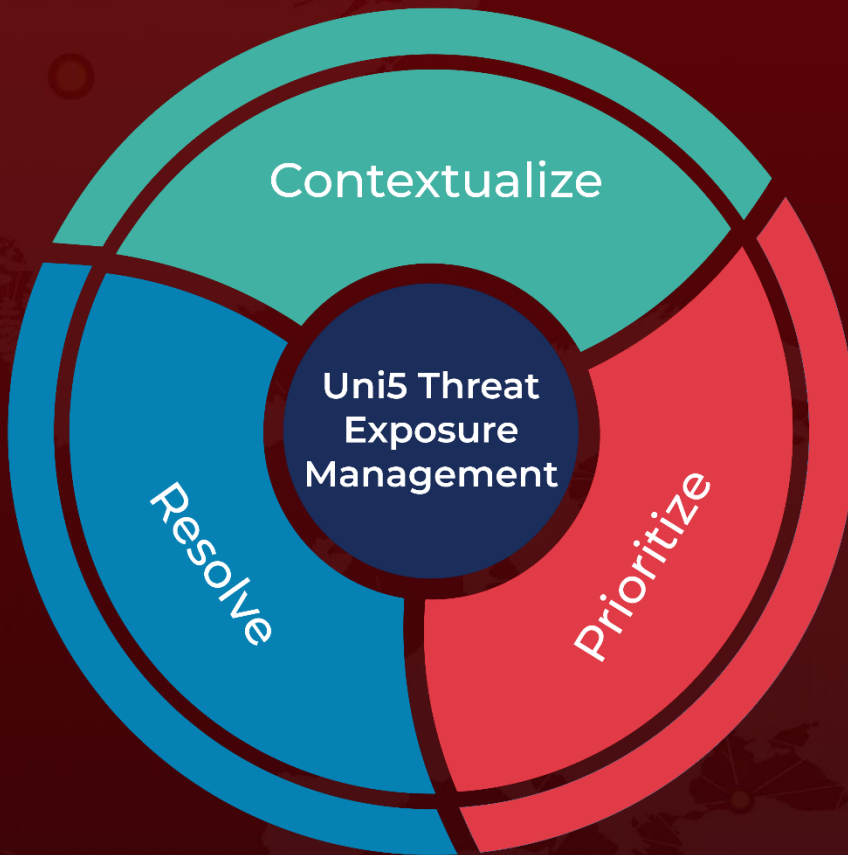
<https://www.cert.ssi.gouv.fr/avis/CERTFR-2024-AVI-0030/>

<https://github.com/Vozec/CVE-2023-7028>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**January 18, 2024 • 4:30 AM**

© 2024 All Rights are Reserved by Hive Pro<sup>®</sup>



More at [www.hivepro.com](http://www.hivepro.com)