Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

GitLab Releases Critical Patch to Address Pipeline Execution Vulnerability

Date of Publication	Admiralty Code	TA Number
September 21, 2023	A1	TA2023380

Summary

Discovered On: September 18, 2023
Affected Product: GitLab Enterprise Edition (EE)
Impact: The critical security vulnerability CVE-2023-5009 affects all versions of GitLab Enterprise Edition (EE). This vulnerability is significant as it enables an attacker to execute pipelines as another user, potentially leading to unauthorized access and misuse of the GitLab environment. This vulnerability represents a bypass of CVE-2023-3932.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2023-5009	GitLab Pipeline Execution Vulnerability	GitLab Enterprise Edition (EE)	✗	✗	✓
CVE-2023-3932	GitLab Pipeline Execution Vulnerability	GitLab Enterprise Edition (EE)	✗	✓	✓

Vulnerability Details

#1 GitLab has released security patches to address a critical vulnerability, CVE-2023-5009, that could allow an attacker to execute pipelines as another user. This vulnerability impacts all versions of GitLab Enterprise Edition (EE) from 13.12 to 16.2.7 and from 16.3 to 16.3.4.

#2 The successful exploitation might provide a threat actor access to confidential data, or they could utilize the impersonated user's permissions to change the source code or launch arbitrary code on the system, both of which could have devastating consequences. This vulnerability serves as a bypass for CVE-2023-3932.

#3 The CVE-2023-3932 also enabled attackers to run pipeline jobs as an arbitrary user via scheduled security scan policies. Threat actors could potentially exploit these flaw for activities such as intellectual property theft, data breaches, and even instigating supply chain attacks.

#4 CVE-2023-3932 was resolved by GitLab in early August 2023. The new vulnerability, CVE-2023-5009, has been addressed in GitLab versions 16.3.4 and 16.2.7. CVE-2023-5009 exists in Instances having Direct transfers and Security Policies features enabled.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-5009	GitLab Enterprise Edition (EE) starting from 13.12 and prior to 16.2.7 as well as from 16.3 and before 16.3.4.	cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*	CWE-284
CVE-2023-3932	GitLab Enterprise Edition (EE) starting from 13.12 and prior to 16.2.7 as well as from 16.3 and before 16.3.4.	cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*	CWE-862

Recommendations

Apply Patch: Install the security patch provided by GitLab to address the CVE-2023-5009 and CVE-2023-3932 vulnerabilities. This patch closes the security gap that allows attackers to exploit the vulnerability.

Workarounds: In situations where upgrading is not immediately possible, disabling one or both features, Direct Transfer and Security Policies, may be necessary to reduce the vulnerability risk.

Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0042** Resource Development	**TA0004** Privilege Escalation	**TA0001** Initial Access
T1068 Exploitation for Privilege Escalation	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1574** Hijack Execution Flow
T1190 Exploit Public-Facing Application			

Patch Details

To patch the critical security vulnerability in GitLab, it's strongly recommended to upgrade to the GitLab Enterprise Edition (EE) versions 16.3.4 and 16.2.7,

Link:
https://about.gitlab.com/releases/2023/09/18/security-release-gitlab-16-3-4-released/#attacker-can-abuse-scan-execution-policies-to-run-pipelines-as-another-user

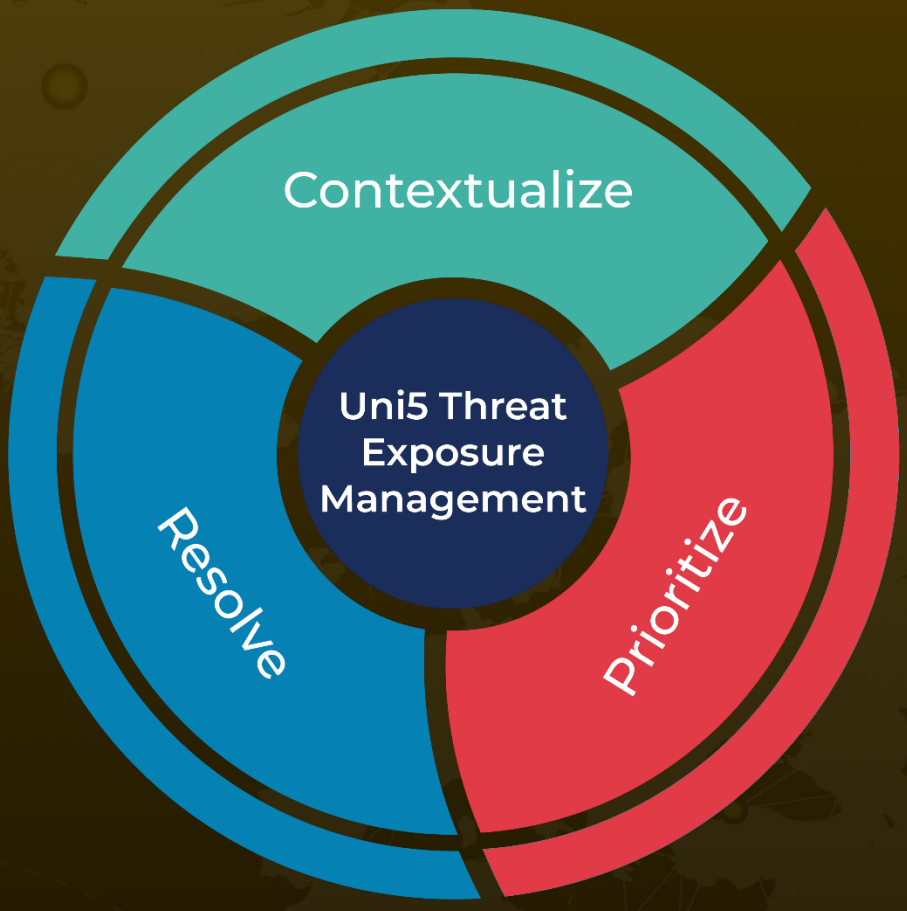
References

https://about.gitlab.com/releases/2023/09/18/security-release-gitlab-16-3-4-released/#attacker-can-abuse-scan-execution-policies-to-run-pipelines-as-another-user

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

September 21, 2023 . 6:55 AM

More at www.hivepro.com