Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

GitLab Addresses Critical Flaws in Community and Enterprise Editions

Date of Publication	Admiralty Code	TA Number
October 11, 2024	A1	TA2024390

Summary

First Seen: October 9, 2024
Affected Products: GitLab Community Edition (CE) and Enterprise Edition (EE)
Impact: GitLab has issued critical security patches addressing multiple vulnerabilities across its Community Edition (CE) and Enterprise Edition (EE). Among these, CVE-2024-9164 is a particularly severe flaw that allows arbitrary branch pipeline execution, potentially enabling attackers to bypass branch protection mechanisms. Exploiting this vulnerability may allow threat actors to execute arbitrary code or gain unauthorized access to sensitive data, compromising the integrity and confidentiality of the system. To protect against these vulnerabilities, users are strongly urged to apply the latest security patches.

⚙ CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2024-9164	GitLab Enterprise Editions Arbitrary Branch Pipeline Vulnerability	GitLab EE	✗	✗	✓
CVE-2024-8970	GitLab Community and Enterprise Editions Arbitrary User Impersonation Vulnerability	GitLab CE/EE	✗	✗	✓
CVE-2024-8977	GitLab Enterprise Editions Server-Side Request Forgery (SSRF) Vulnerability	GitLab EE	✗	✗	✓
CVE-2024-9631	GitLab Community and Enterprise Editions Denial-of-Service (DoS) Vulnerability	GitLab CE/EE	✗	✗	✓
CVE-2024-6530	GitLab Cross-Site Scripting Vulnerability	GitLab	✗	✗	✓

Vulnerability Details

#1 GitLab has issued security updates for both its Community Edition (CE) and Enterprise Edition (EE) to address several critical security vulnerabilities. GitLab, a widely-used open-source platform, plays a central role in DevOps and DevSecOps projects, offering capabilities for code storage, issue tracking, and integrated CI/CD pipelines. Given its importance in modern development workflows, any security vulnerabilities within GitLab pose a serious threat to organizations.

#2 The most critical vulnerability, CVE-2024-9164, affects multiple versions of GitLab Enterprise Edition (EE). This flaw allows malicious actors to execute pipelines on arbitrary branches, potentially gaining unauthorized access to sensitive data and on systems. Exploiting this vulnerability could lead to significant security breaches.

#3 In addition to CVE-2024-9164, several other high-severity vulnerabilities have been addressed in this update. CVE-2024-8970 is a vulnerability that allows attackers to impersonate arbitrary users under certain conditions, enabling unauthorized actions and increasing the risk of data breaches. This flaw could severely compromise the integrity of sensitive information stored in GitLab repositories.

#4 Another notable issue, CVE-2024-8977, involves a Server-Side Request Forgery (SSRF) vulnerability in the Analytics Dashboard. This flaw allows attackers to access internal resources and services, potentially exposing critical infrastructure to exploitation. Furthermore, CVE-2024-9631 poses a risk when viewing code differences in merge requests with conflicts, which can lead to performance slowdowns and a Denial-of-Service (DoS) condition, disrupting development workflows.

#5 Lastly, CVE-2024-6530 is an XSS vulnerability that causes HTML injection on the OAuth page when authorizing new applications, enabling attackers to inject malicious scripts and potentially compromise both user data and the overall integrity of a web application. To protect against these vulnerabilities, users are strongly urged to apply the latest security patches. Upgrading to the recommended versions will ensure that systems remain secure and protected from potential exploitation, safeguarding both the data and integrity of GitLab environments.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-9164	GitLab EE versions starting from 12.5 prior to 17.2.9, starting from 17.3, prior to 17.3.5, and starting from 17.4 prior to 17.4.2	cpe:2.3:a:gitlab:gitlab-ee:*:*:*:*:*:*:*	CWE-284
CVE-2024-8970	GitLab CE/EE versions starting from 11.6 prior to 17.2.9, starting from 17.3 prior to 17.3.5, and starting from 17.4 prior to 17.4.2	cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:* cpe:2.3:a:gitlab:gitlab-ee:*:*:*:*:*:*:*	CWE-284
CVE-2024-8977	GitLab EE versions starting from 15.10 prior to 17.2.9, from 17.3 prior to 17.3.5, and from 17.4 prior to 17.4.2	cpe:2.3:a:gitlab:gitlab-ee:*:*:*:*:*:*:*	CWE-918
CVE-2024-9631	GitLab CE/EE versions starting from 13.6 prior to 17.2.9, starting from 17.3 prior to 17.3.5, and starting from 17.4 prior to 17.4.2	cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:* cpe:2.3:a:gitlab:gitlab-ee:*:*:*:*:*:*:*	CWE-20
CVE-2024-6530	GitLab versions starting from 17.1 prior 17.2.9, starting from 17.3 prior to 17.3.5, and starting from 17.4 prior to 17.4.2	cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:* cpe:2.3:a:gitlab:gitlab-ee:*:*:*:*:*:*:*	CWE-79

Recommendations

Upgrade Immediately: All GitLab users are strongly urged to update immediately, as patches addressing the vulnerabilities have been released in versions 17.4.2, 17.3.5, and 17.2.9. It is critical that all installations running affected versions are upgraded to the latest release to ensure protection against potential threats and security risks.

Review CI/CD Permissions: Conduct an audit of your GitLab repositories and pipelines. Limit access to trusted users who require it. Misconfigured permissions can allow malicious users to trigger pipelines, potentially leading to unauthorized execution of code. Ensure that CI/CD is restricted to appropriate branches and contributors.

Implement Network Segmentation: Use network segmentation to limit access to sensitive internal resources and services. This can help contain any potential exploitation from the vulnerabilities and minimize the impact of any security incidents.

Monitor for Anomalies: Implement monitoring solutions to detect unusual activities within the GitLab environment. Pay special attention to user impersonation attempts and unauthorized actions, as these could indicate exploitation of vulnerabilities.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0011** Command and Control
TA0040 Impact	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1190** Exploit Public-Facing Application
T1059 Command and Scripting Interpreter	**T1203** Exploitation for Client Execution	**T1090** Proxy	**T1499** Endpoint Denial of Service

Patch Details

Users are strongly advised to update to the latest security patches, specifically versions 17.4.2, 17.3.5, and 17.2.9, for both GitLab Community Edition (CE) and Enterprise Edition (EE). These versions effectively address and resolve the identified vulnerabilities, ensuring that systems are protected from potential exploitation.

Link: https://gitlab.com/gitlab-org/gitlab/-/releases

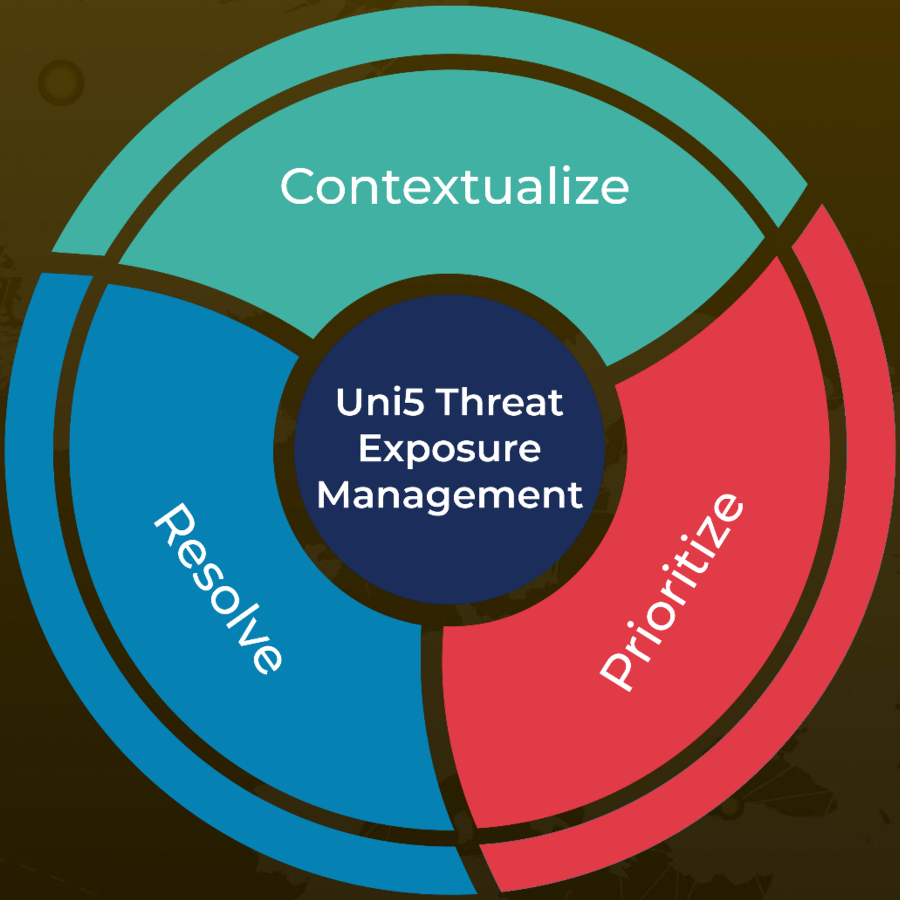
References

https://about.gitlab.com/releases/2024/10/09/patch-release-gitlab-17-4-2-released/

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

October 11, 2024 • 6:20 AM

More at www.hivepro.com