Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

GitLab Flaw Allows Account Takeover via XSS Attacks

Date of Publication	Admiralty Code	TA Number
May 24, 2024	A1	TA2024207

Summary

Discovered: May 2024
Affected Products: GitLab
Impact: GitLab has addressed a high-severity vulnerability identified as CVE-2024-4835, which allowed unauthenticated attackers to take over user accounts through cross-site scripting (XSS) attacks. This XSS vulnerability was found in the VS code editor (Web IDE) integrated within GitLab.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-4835	GitLab XSS Condition Vulnerability	GitLab	✗	✗	✓

Vulnerability Details

#1 GitLab has resolved a high-severity vulnerability identified as CVE-2024-4835. This vulnerability allowed unauthenticated attackers to take over user accounts through cross-site scripting (XSS) attacks. The XSS flaw was discovered in the VS Code editor (Web IDE) integrated within GitLab, enabling 1-click account takeover via XSS.

#2 The vulnerability stemmed from how the VS Code editor (Web IDE) handled certain inputs. Attackers could craft malicious pages that, when accessed by a GitLab user, executed arbitrary scripts in the user's browser. This could lead to unauthorized access to the user's account and data.

#3 This vulnerability could be exploited to Steal restricted information, take over user accounts by executing arbitrary scripts within the user's session context, perform actions on behalf of the user without their knowledge, including accessing sensitive data and modifying repository contents.

#4 CVE-2024-4835 underscores the importance of securing web applications against XSS vulnerabilities, particularly those exploitable without authentication. Another Gitlab Account takeover vulnerability, **CVE-2023-7028**, is currently being exploited and has recently been added to the CISA KEV catalog. Users are strongly encouraged to promptly update their GitLab installations to the latest version to ensure protection against these vulnerabilities.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-4835	GitLab versions 15.11 prior to 16.10.6, 16.11 prior to 16.11.3, and 17.0 prior to 17.0.1.	cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:*	CWE-79

Recommendations

Update GitLab Instances: Ensure that all GitLab installations are updated to the latest versions that include the patch for CVE-2024-4835.

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.

Network Segmentation: Implement network segmentation to isolate critical infrastructure components from other systems. This can limit lateral movement for attackers and contain potential breaches.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0010 Exfiltration
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter	T1059.005 Visual Basic
T1204 User Execution	T1204.001 Malicious Link	T1566 Phishing	T1189 Drive-by Compromise

Patch Details

GitLab has released a patch to fix the vulnerability in the latest version 17.0.1, 16.11.3, 16.10.6 for GitLab Community Edition (CE) and Enterprise Edition (EE).

Links:
https://about.gitlab.com/releases/2024/05/22/patch-release-gitlab-17-0-1-released/#1-click-account-takeover-via-xss-leveraging-the-vs-code-editor-web-ide

References

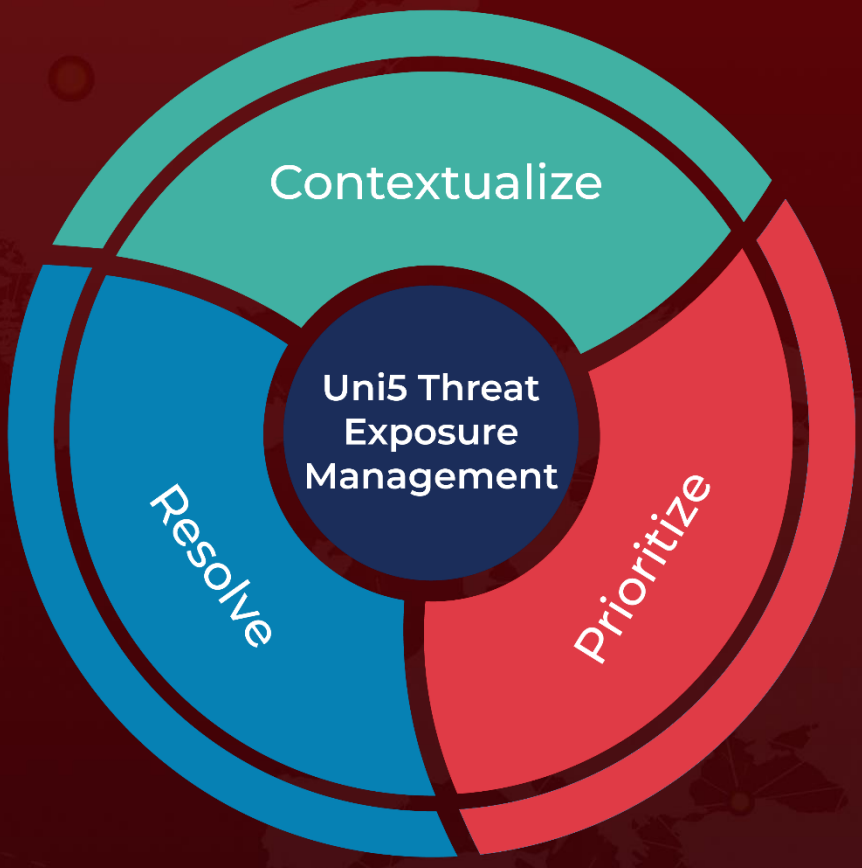
https://about.gitlab.com/releases/2024/05/22/patch-release-gitlab-17-0-1-released/#1-click-account-takeover-via-xss-leveraging-the-vs-code-editor-web-ide

https://www.hivepro.com/threat-advisory/gitlab-fixes-critical-account-takeover-vulnerability/

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

May 24, 2024 • 6:00 AM

More at www.hivepro.com