

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

GitLab releases new CE and EE versions to address integer overflow vulnerabilities

Date of Publication

January 19, 2023

Admiralty code

A1

TA Number

TA2023031



Summary

First Seen: January 17, 2023

Affected Product: GitLab

Impact: Remote code execution

CVEs

CVE	NAME	PATCH
CVE-2022-41903	Arbitrary Heap Write	
CVE-2022-23521	Arbitrary Heap Read and Write	

Vulnerability Details

The GitLab CE and EE have two security issues in Git. One of them is CVE-2022-41903, which is an integer overflow in the `'git-log'` and `'git-archive'` commands that can result in arbitrary heap writes and remote code execution. Additionally, there is another security issue named CVE-2022-23521, which is an integer overflow in `'gitattributes'` that can result in arbitrary heap reads and writes, and remote code execution.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-41903	Gitlab Community Edition: 15.0.0 - 15.7.4	cpe:2.3:a:gitlab:gitlab: *:*:*:community:*: :*	CWE-122
CVE-2022-23521	GitLab Enterprise Edition: 15.0.0 - 15.7.3	cpe:2.3:a:gitlab:gitlab: *:*:*:enterprise:*:*: *	CWE- 20

Recommendations



Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.



Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Patch Details' on the following page.

Patch Details

Update GitLab Community Edition (CE) and Enterprise Edition (EE) to 15.7.5, 15.6.6, and 15.5.9

Patch Link

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

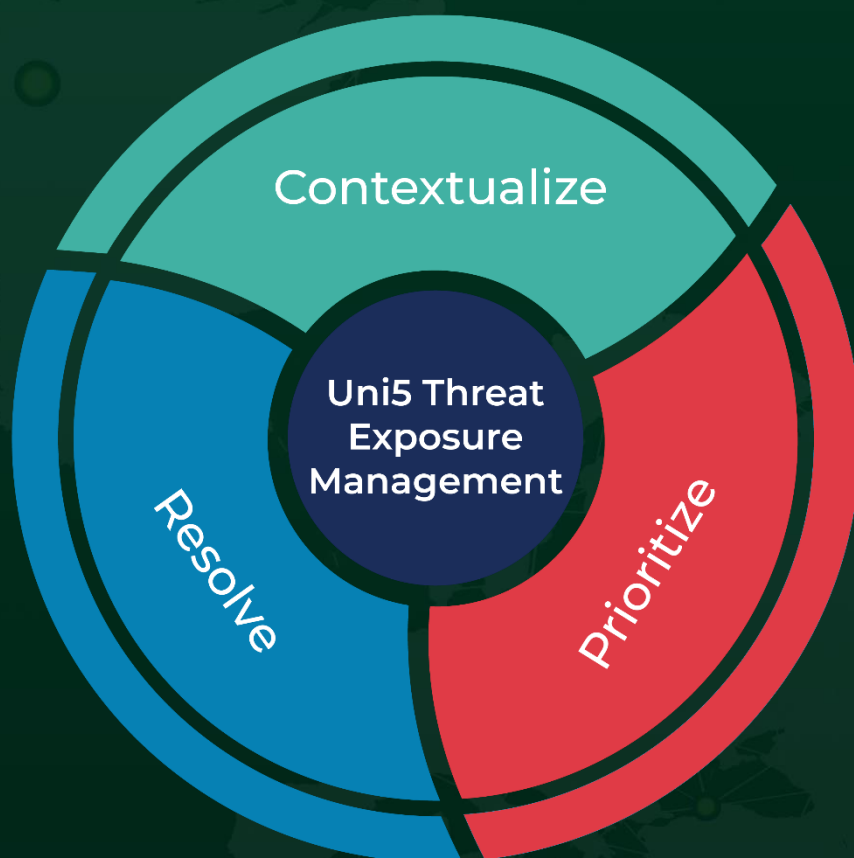
References

<https://about.gitlab.com/releases/2023/01/17/critical-security-release-gitlab-15-7-5-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

January 19, 2023 • 12:25 PM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com