Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

‘Looney Tunables’ Flaw Enables Local Privilege Escalation in Glibc

Date of Publication	Admiralty Code	TA Number
October 4, 2023	A1	TA2023396

Summary

First Seen: September 4, 2023
Affected Platform: Linux
Impact: The CVE-2023-4911 aka Looney Tunables is a buffer overflow vulnerability in the glibc's dynamic loader (ld.so). The vulnerability can be exploited by a local user to gain root privileges on the system.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2023-4911	Glibc Buffer Overflow Vulnerability	GNU C Library (glibc)	✗	✓	✓

Vulnerability Details

#1 CVE-2023-4911, also known as "Looney Tunables," is a critical buffer overflow vulnerability discovered in the GNU C Library's dynamic loader, specifically in the processing of the GLIBC_TUNABLES environment variable. This vulnerability, which was introduced in April 2021, poses a significant security risk to various Linux distributions, including Fedora, Ubuntu, and Debian.

#2 The GLIBC_TUNABLES environment variable allows users to adjust the behavior of the GNU C Library at runtime without the need for recompilation. If exploited, this vulnerability can have adverse effects on system performance, reliability, and security. The vulnerability enables local privilege escalation, potentially granting an attacker full root privileges on the affected Linux system.

#3 It is crucial to address this issue promptly to safeguard system integrity and security. Notably, some Linux distributions like Alpine Linux are unaffected due to their use of musl libc, but many widely-used distributions could be vulnerable.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-4911	All systems running glibc 2.34 to 2.37	cpe:2.3:a:gnu:c_library:*:*:*:*:*:*:*:*	CWE-120

Recommendations

Apply Security Patches: Immediately apply security patches provided by your Linux distribution's vendor or upstream provider to address the CVE-2023-4911 vulnerability. Regularly check for updates and ensure that your systems are running the latest software versions.

Update GLIBC: Ensure that the GNU C Library (GLIBC) on your systems is updated to a patched version that addresses the buffer overflow vulnerability. Follow best practices for library management.

Vulnerability Assessment: Conduct a thorough vulnerability assessment to identify affected systems in your environment. This can help you prioritize patching efforts and ensure all vulnerable systems are addressed.

Potential MITRE ATT&CK TTPs

TA0004 Privilege Escalation	TA0042 Resource Development	TA0002 Execution	T1588.006 Vulnerabilities
T1068 Exploitation for Privilege Escalation	T1588 Obtain Capabilities	T1588.005 Exploits	

Patch Details

Upgrade glibc to 2.38 or later versions

References

https://www.qualys.com/cve-2023-4911/

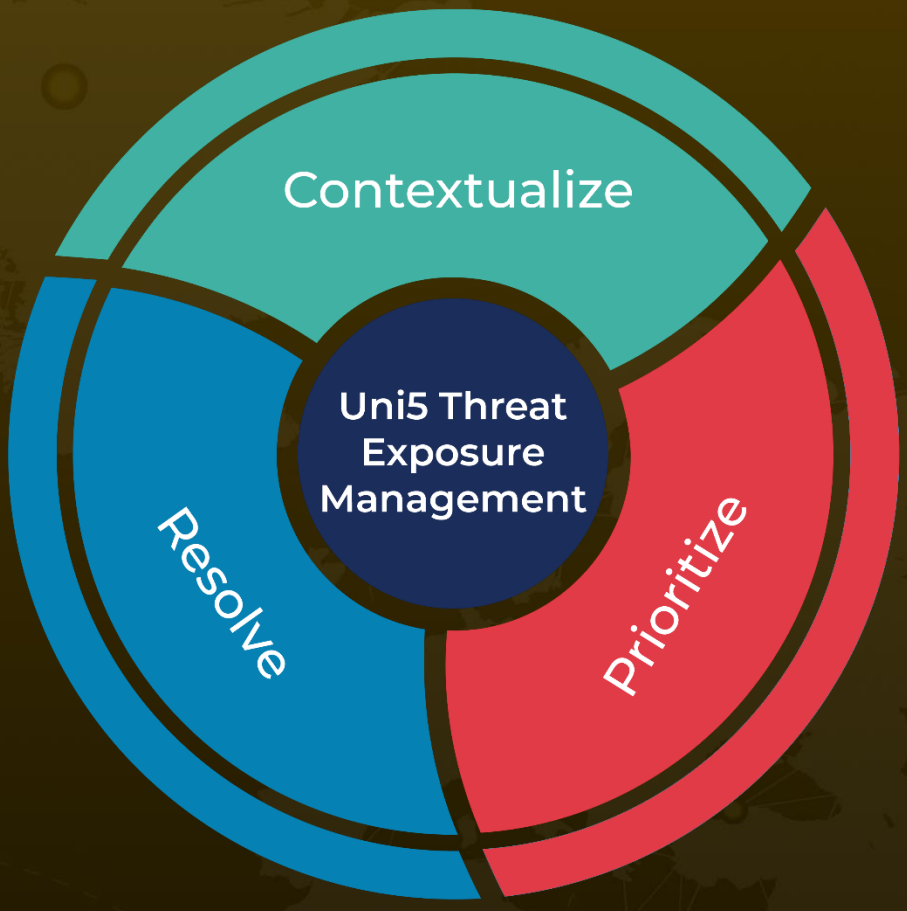
https://www.qualys.com/2023/10/03/cve-2023-4911/looney-tunables-local-privilege-escalation-glibc-ld-so.txt

https://access.redhat.com/security/cve/CVE-2023-4911

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 4, 2023 . 07:30 AM

More at www.hivepro.com