Hive Pro®

Threat Level

Amber

HiveForce Labs

# THREAT ADVISORY

## VULNERABILITY REPORT

# GNOME Linux Systems Exposed to 1-Click RCE Attacks

| Date of Publication | Admiralty Code | TA Number |
|---|---|---|
| October 10, 2023 | A1 | TA2023407 |

# Summary

**First Discovered:** October 9, 2023
**Affected Product:** GNOME
**Affected Platform:** Linux
**Impact:** A new security vulnerability, known as CVE-2023-43641, has been identified in the libcue library. This library is utilized by Tracker Miners and is shipped along with the GNOME desktop environment. This vulnerability presents a significant threat to Linux systems using the GNOME Desktop environment, as successful exploitation could result in arbitrary code execution.

## CVEs

| CVE | NAME | AFFECTED PRODUCTS | ZERO-DAY | CISA | PATCH |
|---|---|---|---|---|---|
| CVE-2023-43641 | libcue Arbitrary code execution Vulnerability | GNOME, libcue | ✗ | ✗ | ✓ |

# Vulnerability Details

**#1** CVE-2023-43641 is a memory corruption vulnerability found in the open-source libcue library. It can potentially allow attackers to execute arbitrary code on Linux systems that run the GNOME desktop environment.

**#2** The libcue library is integrated into Tracker Miners, which is a search engine tool that comes pre-installed in GNOME. Tracker Miners are responsible for indexing files in the system, making it easier for users to access and search for their files.

**#3** The issue at the core of CVE-2023-43641 lies in an out-of-bounds array access within the track_set_index function. This vulnerability can be exploited to achieve code execution on a target system by luring a victim into clicking on a malicious link that triggers the download of a .cue file.

**#4** The exploitation of CVE-2023-43641 occurs because when the downloaded file with a .cue extension is saved to the user's ~/Downloads directory, it is automatically scanned by tracker-miners. Since the file has the .cue extension, tracker-miners employs libcue to parse the file. The malicious file then exploits the vulnerability in libcue to achieve code execution.

**#5** An attacker can exploit this vulnerability with relative ease. All it takes is for a user to inadvertently click on a malicious link, which can trigger the execution of code on their computer. Therefore, it's essential to be cautious and ensure your system is patched to protect against potential attacks that might target this vulnerability.

## Vulnerability

| CVE ID | AFFECTED PRODUCTS | AFFECTED CPE | CWE ID |
|---|---|---|---|
| CVE-2023-43641 | libcue Versions 2.2.1 and prior | cpe:2.3:a:gnome:libcue_library:*:*:*:*:*:*:*:* | CWE-787 |

# Recommendations

**Update GNOME:** To address the vulnerability, check with package provider for the fixed GNOME version. Update your GNOME desktop environment to the fixed version and also, ensure all system packages are kept up to date.

**Robust Endpoint Security:** Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent vulnerabilities from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

**Be Cautious with Web Links:** Avoid clicking on dubious links or visiting untrusted websites, as they might harbor malicious content. Exercise prudence while interacting with web links in emails or messages from unfamiliar sources, as they could be phishing attempts or contain a malicious exploit like libcue exploit, which could result in arbitrary code execution.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| **TA0042**<br>Resource Development | **TA0001**<br>Initial Access | **TA0002**<br>Execution | **T1204**<br>User Execution |
| **T1588**<br>Obtain Capabilities | **T1588.006**<br>Vulnerabilities | **T1566**<br>Phishing | **T1566.002**<br>Spearphishing Link |
| **T1204.001**<br>Malicious Link | | | |

## Patch Details

Ubuntu has released packages to address this vulnerability for specific versions of their operating system. Update your systems packages with the fixed versions.

Link:
https://launchpad.net/ubuntu/+source/libcue/2.2.1-4ubuntu0.1
https://launchpad.net/ubuntu/+source/libcue/2.2.1-3ubuntu0.1
https://launchpad.net/ubuntu/+source/libcue/2.2.1-2ubuntu0.1

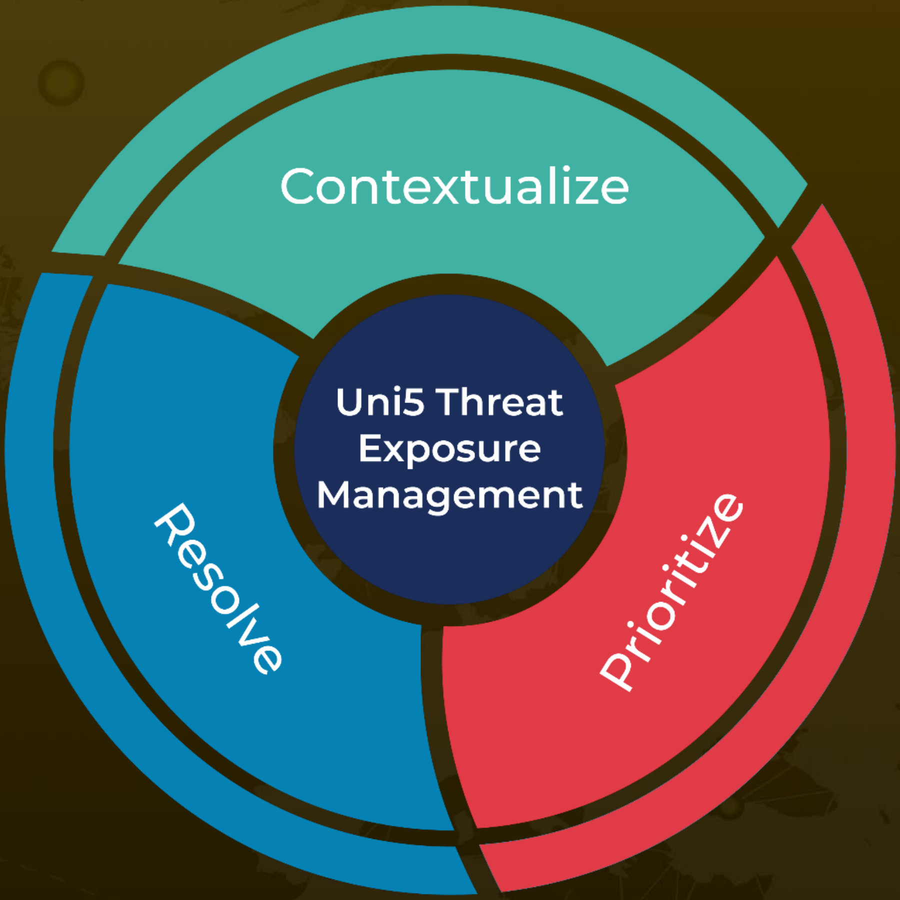
## References

https://github.blog/2023-10-09-coordinated-disclosure-1-click-rce-on-gnome-cve-2023-43641/

# 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 10, 2023 • 9:35 PM**

More at www.hivepro.com