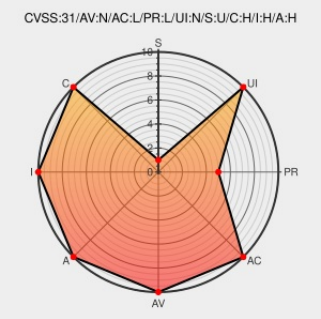
CVE-2023-30844

Published on: Not Yet Published

Last Modified on: 05/15/2023 06:07:00 PM UTC

CVE-2023-30844 - advisory for GHSA-jmp2-wc4p-wfh2

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mutagen from Mutagen contain the following vulnerability:

Mutagen provides real-time file synchronization and flexible network forwarding for developers. Prior to versions 0.16.6 and 0.17.1 in `mutagen` and prior to version 0.17.1 in `mutagen-compose`, Mutagen `list` and `monitor` commands are susceptible to control characters that could be provided by remote endpoints. This could cause terminal corruption, either intentional or unintentional, if these characters were present in error messages or file paths/names. This could be used as an attack vector if synchronizing with an untrusted remote endpoint, synchronizing files not under control of the user, or forwarding to/from an untrusted remote endpoint. On very old systems with terminals susceptible to issues such as CVE-2003-0069, the issue could theoretically cause code execution. The problem has been patched in Mutagen v0.16.6 and v0.17.1. Earlier versions of Mutagen are no longer supported and will not be patched. Versions of Mutagen after v0.18.0 will also have the patch merged. As a workaround, avoiding synchronization of untrusted files or interaction with untrusted remote endpoints should mitigate any risk.

CVE-2023-30844 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **mutagen-io** - **mutagen** version = **github.com/mutagen-io/mutagen < 0.16.6**

Affected Vendor/Software: **mutagen-io** - **mutagen** version = **github.com/mutagen-io/mutagen >= 0.17.0, < 0.17.1**

Affected Vendor/Software: **mutagen-io** - **mutagen** version = **github.com/mutagen-io/mutagen-compose < 0.17.1**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Mutagen command line and logging operations do not neutralize control characters in text controlled by remote endpoints · Advisory · mutagen-io/mutagen · GitHub	github.com text/html	MISC github.com/mutagen-io/mutagen/security/advisories/GHSA-jmp2-wc4p-wfh2
Release v0.16.6 · mutagen-io/mutagen · GitHub	github.com text/html	MISC github.com/mutagen-io/mutagen/releases/tag/v0.16.6
Release v0.17.1 · mutagen-io/mutagen · GitHub	github.com text/html	MISC github.com/mutagen-io/mutagen/releases/tag/v0.17.1

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mutagen	Mutagen	All	All	All	All
Application	Mutagen	Mutagen	0.17.0	All	All	All
Application	Mutagen	Mutagen Compose	All	All	All	All

cpe:2.3:a:mutagen:mutagen:*:*:*:*:*:*:*:*:

cpe:2.3:a:mutagen:mutagen:0.17.0:*:*:*:*:*:*:*:

cpe:2.3:a:mutagen:mutagen_compose:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@threatmeter	CVE-2023-30844 | mutagen Control Character neutralization A vulnerability, which was classified as problematic, has… twitter.com/i/web/status/1…	2023-05-05 07:51:11
@CVEreport	CVE-2023-30844 : Mutagen provides real-time file synchronization and flexible network forwarding for developers. Pr… twitter.com/i/web/status/1…	2023-05-08 18:07:27

← Previous ID

Next ID→

© CVE.report 2023 | Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report