

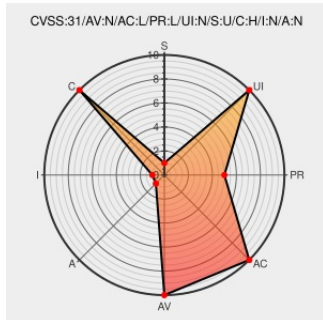


CVE-2023-27587

Published on: Not Yet Published

Last Modified on: 03/17/2023 04:26:00 PM UTC

CVE-2023-27587 - advisory for GHSA-23g5-r34j-mr8g

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Readtomyshee](#) from [Readtomyshee Project](#) contain the following vulnerability:

ReadtoMyShoe, a web app that lets users upload articles and listen to them later, generates an error message containing sensitive information prior to commit 8533b01. If an error occurs when adding an article, the website shows the user an error message. If the error originates from the Google Cloud TTS request, then it will include the

full URL of the request. The request URL contains the Google Cloud API key. This has been patched in commit 8533b01. Upgrading should be accompanied by deleting the current GCP API key and issuing a new one. There are no known workarounds.

CVE-2023-27587 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [rozbb](#) - [readtomyshee](#) version = <= 0.2.0

CVSS3 Score: **6.5 - MEDIUM**

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

CVE References

Description	Tags	Link
API key leak · Advisory · rozbb/readtomyshee · GitHub	github.com text/html	MISC github.com/rozbb/readtomyshee/security/advisories/GHSA-23g5-r34j-mr8g
Fixed leakage of GCP API key through TTS error message · rozbb/readtomyshee@8533b01 · GitHub	github.com text/html	MISC github.com/rozbb/readtomyshee/commit/8533b01c818939a0fa919c7244d8dbf5daf032af

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

Exploit/POC from Github

The simple PoC of CVE-2023-27587

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Readtomys Shoe Project	Readtomys shoe	All	All	All	All
cpe:2.3:a:readtomys shoe_project:readtomys shoe:*****:.*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-27587 : ReadtoMyShoe, a web app that lets users upload articles and listen to them later, generates an err... twitter.com/i/web/status/1...	2023-03-13 22:02:35
 /r/netcve	CVE-2023-27587	2023-03-13 22:38:39
 /r/Team_IT_Security	CVE-2023-27587 ReadtoMyShoe information exposure (GHSA-23g5-r34j-mr8g)	2023-04-07 06:40:10

[← 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 registered 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](#)