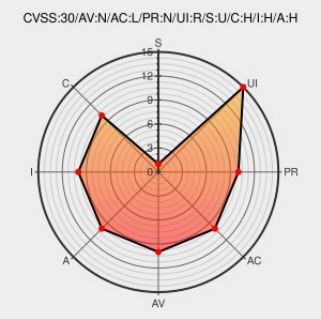
CVE-2018-1000843

Published on: 12/20/2018 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:51:00 AM UTC

CVE-2018-1000843

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



Certain versions of Luigi from Spotify contain the following vulnerability:

Luigi version prior to version 2.8.0; after commit 53b52e12745075a8acc016d33945d9d6a7a6aaeb; after GitHub PR spotify/luigi/pull/1870 contains a Cross ite Request Forgery (CSRF) vulnerability in API endpoint: /api/<method> that can result in Task metadata such as task name, id, parameter, etc. will be leaked to unauthorized users. This attack appear to be exploitable via The victim must visit a specially crafted webpage from the network where their Luigi server is accessible.. This vulnerability appears to have been fixed in 2.8.0 and later.

CVE-2018-1000843 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Add CORS headers to api requests by jessiecoustin · Pull	Exploit	MISC:github.com/spotify/luigi/pull/1870

Add CORS headers to api requests by jessicaaustin · Pull Request #1870 · spotify/luigi · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/spotify/luigi/pull/1870
luigi/server.py at 2.7.9 · spotify/luigi · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/spotify/luigi/blob/2.7.9/luigi/server.py#L67
Google Groups	groups.google.com text/html	MISC groups.google.com/forum/#!topic/luigi-user/ZgfRTpBsVUY

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.

Related QID Numbers

980968 Python (pip) Security Update for luigi (GHSA-p69g-f978-xxv9)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Spotify	Luigi	All	All	All	All
Application	Spotify	Luigi	All	All	All	All

cpe:2.3:a:spotify:luigi:*:*:*:*:*:*:*:*:

cpe:2.3:a:spotify:luigi:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→