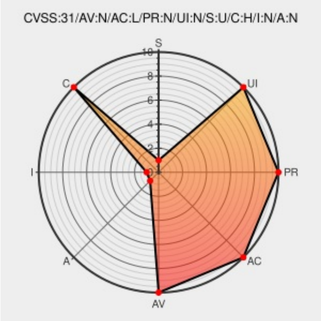
CVE-2021-41077

Published on: 09/14/2021 12:00:00 AM UTC

Last Modified on: 09/29/2021 06:37:00 PM UTC

CVE-2021-41077

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Travis Ci from Travis-ci contain the following vulnerability:

The activation process in Travis CI, for certain 2021-09-03 through 2021-09-10 builds, causes secret data to have unexpected sharing that is not specified by the customer-controlled .travis.yml file. In particular, the desired behavior (if .travis.yml has been created locally by a customer, and added to git) is for a Travis service to perform builds in a way that prevents public access to customer-specific secret environment data such as signing keys, access credentials, and API tokens. However, during the stated 8-day interval, secret data could be revealed to an unauthorized actor who forked a public repository and printed files during a build process.

CVE-2021-41077 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
JavaScript is not available.	nitter.domain.glass text/html	MISC twitter.com/peter_szilagyi/status/1437649838477283330
The Travis CI Blog: Security Bulletin	blog.travis-ci.com text/html	MISC blog.travis-ci.com/2021-09-13-bulletin
Travis CI Leaked Secure Environment Variables | Hacker News	news.ycombinator.com text/html	MISC news.ycombinator.com/item?id=28523350
Security Bulletin - Announcements - Travis CI Community	travis-ci.community text/html	MISC travis-ci.community/t/security-bulletin/12081
Péter Szilágyi (karalabe.eth) on Twitter: "Between the 3 Sept and 10 Sept, secure env vars of *all* public @travisci repositories were injected into PR builds. Signing keys, access creds, API tokens. Anyone could exfiltrate these and gain lateral movement into 1000s of orgs. #security 1/4 https://t.co/i23jFzAjjH"	nitter.domain.glass text/html	MISC twitter.com/peter_szilagyi/status/1437646118700175360
Secure env vars of all public travisci repositories were injected into PR builds | Hacker News	news.ycombinator.com text/html	MISC news.ycombinator.com/item?id=28524727

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

PoC for exploiting CVE-2021-41077 : The activation process in Travis CI, for certain 2021-09-03 through 2021-09-10 bu…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Travis-ci	Travis Ci	All	All	All	All

cpe:2.3:a:travis-ci:travis_ci:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-41077 : The activation process in Travis CI, for certain 2021-09-03 through 2021-09-10 builds, causes secr… twitter.com/i/web/status/1…	2021-09-14 15:43:00
@azu_re	CVEが登録されてた。 "CVE - CVE-2021-41077"	2021-09-14 15:53:34
@alexanderjaeger	And also a CVE has been assigned: @CVEnew #CVE202141077	2021-09-15 08:44:20

@alexanderjaeger		[illegible]
@_lijnk	@Jeremy_Kirk @peter_szilagyi	2021-09-15 14:33:30
@autumn_good_35	CVE-2021-41077 Travis CI Flaw Exposes Secrets of Thousands of Open Source Projects thehackernews.com/2021/09/travis…	2021-09-16 15:10:13
@wallofsheep	#Travis CI Flaw exposes secrets of thousands of #opensource projects! CVE-2021-41077 - fork a public repo with a p… twitter.com/i/web/status/1…	2021-09-16 18:50:02
@HackersOmhe	Error de ciberseguridad en Travis CI	2021-09-17 03:46:39
@eagerbeavertech	thehackernews.com/2021/09/travis… The issue - tracked as CVE-2021-41077 - concerns unauthorized access and plunder of sec… twitter.com/i/web/status/1…	2021-09-17 04:03:32
@eed3si9n	due to the poor handling of the recent security incident CVE-2021-41077, I'm suspending Travis CI integration on al… twitter.com/i/web/status/1…	2021-09-19 02:40:49
@sickcodes	Travis CI’s advisory for CVE-2021-41077 is ~45 words of blaming the victims of their own vulnerability. The adviso… twitter.com/i/web/status/1…	2021-09-19 08:13:48
@kabukawa	CVE-2021-41077	2021-09-19 11:10:33

← Previous ID

Next ID→

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