ROTATE YOUR SEC

Travis C usands of open

Developers furious at Travis CI's "insanely embarrassing 'security bulletin.'"

AX SHARMA - 9/14/2021, 9:12 PM

Getty Images

Enlarge

A security flaw in Travis CI potentially exposed the secrets of thousands of open source projects that rely on the hosted continuous integration service. Travis CI is a software-testing solution used by over 900,000 open source projects and 600,000 users. A vulnerability in the tool made it possible for secure environment variables—signing keys, access credentials, and API tokens of all public open source projects—to be exfiltrated.

Worse, the dev com sure process and the brief "secu

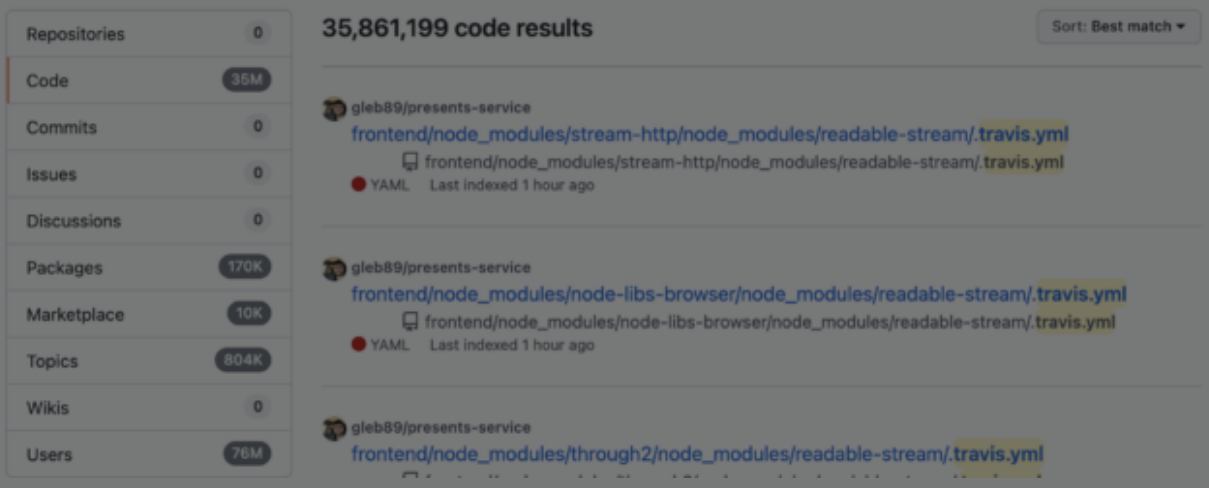
Environme st builds

Travis CI is a popula and Bitbucket. As the makers of th

> When you run irtual environment a more of those tasks fail s considered passed and Tra

But this month, researcher Felix Lange found a security vulnerability that caused Travis CI to include secure environment variables of *all* public open source repositories that use Travis CI into pull request builds. Environment variables can include sensitive secrets like signing keys, access credentials, and API tokens. If these variables are exposed, attackers can abuse the secrets to obtain lateral movement into the networks of thousands of organizations.

A simple GitHub search demonstrates that Travis is in widespread use by a large number of projects:



Enlarge / GitHub search results for "travis.yml."

Tracked as CVE-2021-41077, the bug is present in Travis CI's activation process and impacts certain builds created between September 3 and September 10. As a part of this activation process,

developers are supposed to add a ".travis.yml" file to their open source project repository. This file tells Travis CI what to do and may contain encrypted secrets. Another place encrypted secrets may be defined is Travis' web UI. But, these secrets are not meant to be exposed. In fact, Travis CI's docs have always stated, "Encrypted environment variables are not available to pull requests from forks due to the security risk of exposing such information to unknown code."

Ideally, Travis is exp[illegible]environment variables specified.

"These secure environment variables... are configured on Travis' web UI and remain in Travis' sole possession," Péter Szilágyi, Ethereum cryptocurrency project lead told Ars. "Those variables then get added to the environment in which builds are running, but only for trusted code (i.e. code that has been merged). For external code (PRs), the env vars should not be inserted, since the maintainer has no control over the code that outsiders submit. The problem was that they messed something up and ended up injecting the secret keys into untrusted builds too."

This vulnerability caused these sorts of secrets to be unexpectedly exposed to just about anyone forking a public repository and printing files during a build process.

Fortunately, the issue didn't last too long—around eight days, thanks to Lange and other researchers who notified the company of the bug on September 7. But out of caution, all projects relying on Travis CI are advised to rotate their secrets.

While not exactly similar in nature, the vulnerability has echoes of the Codecov supply chain attack in which threat actors had exfiltrated secrets and sensitive environment variables of many Codecov customers from their CI/CD environments, leading to further data leaks at prominent companies.

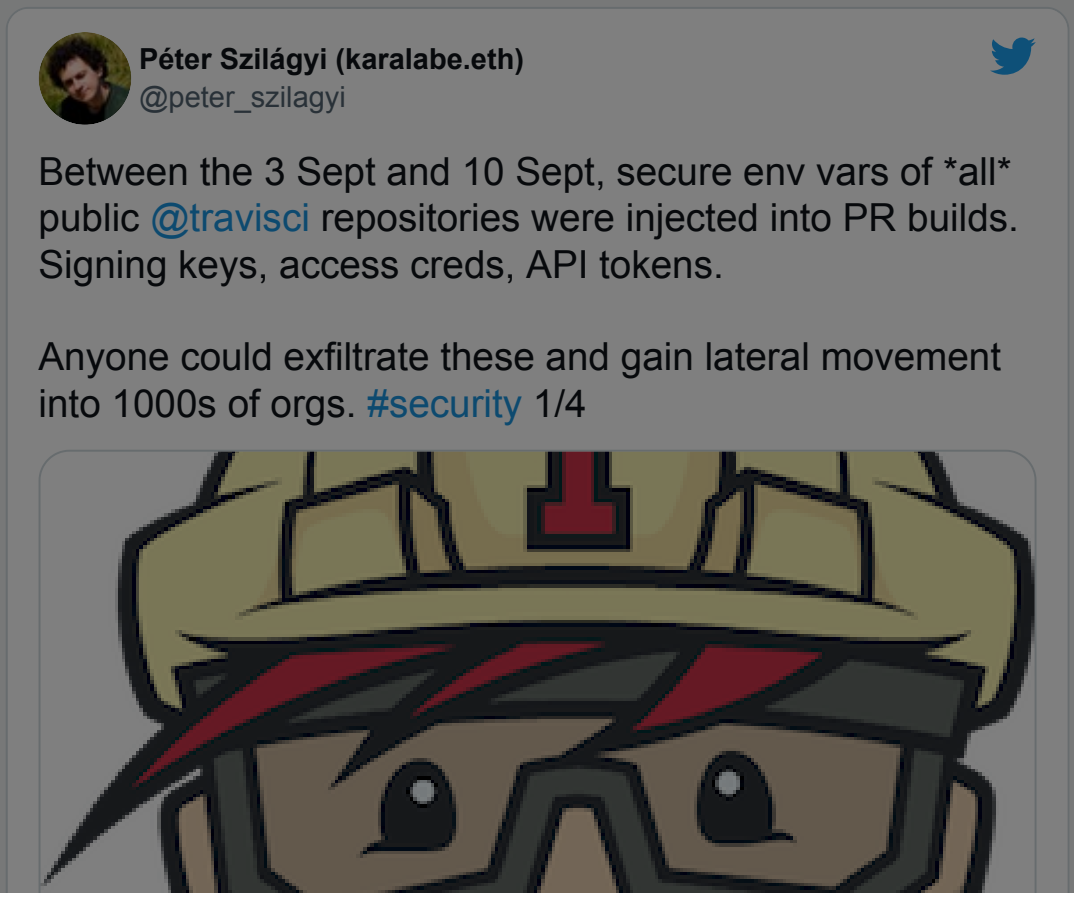
"According to a received report, a public repository forked from another one could file a pull request (standard functionality, e.g., in GitHub, BitBucket, Assembla) and while doing it obtain unauthorized access to secrets from the original public repository with a condition of printing some of the files during the build process," explained Montana Mendy of Travis CI in a security bulletin. "In this scenario, secrets are still encrypted in the Travis CI database."

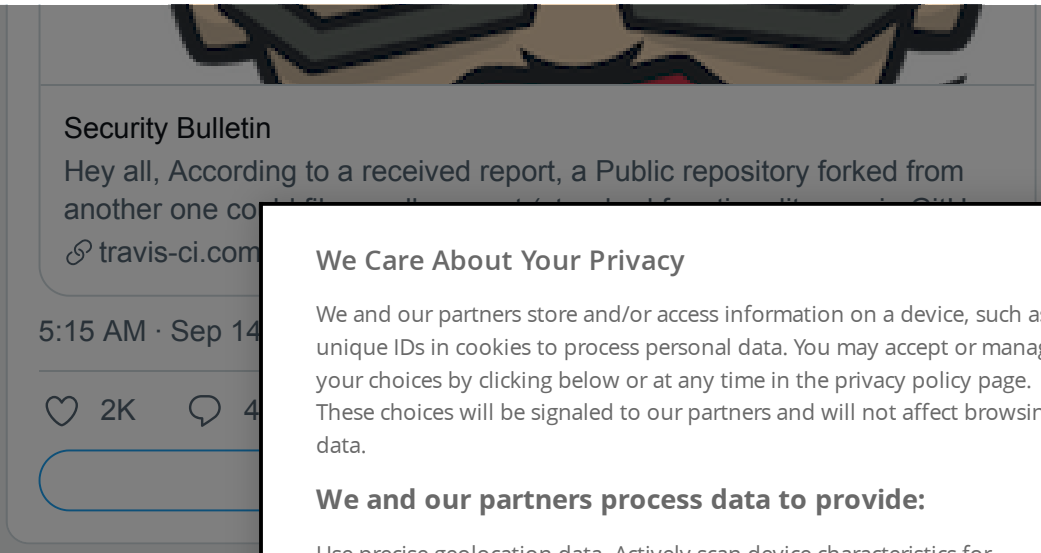
Mendy says the issue only applies to public repositories and not to private repositories, as repository owners of the latter have full control over who can fork their repositories.

Community furious over flimsy “security bulletin”

The presence and r y bulletin and overall handling of mmunity.

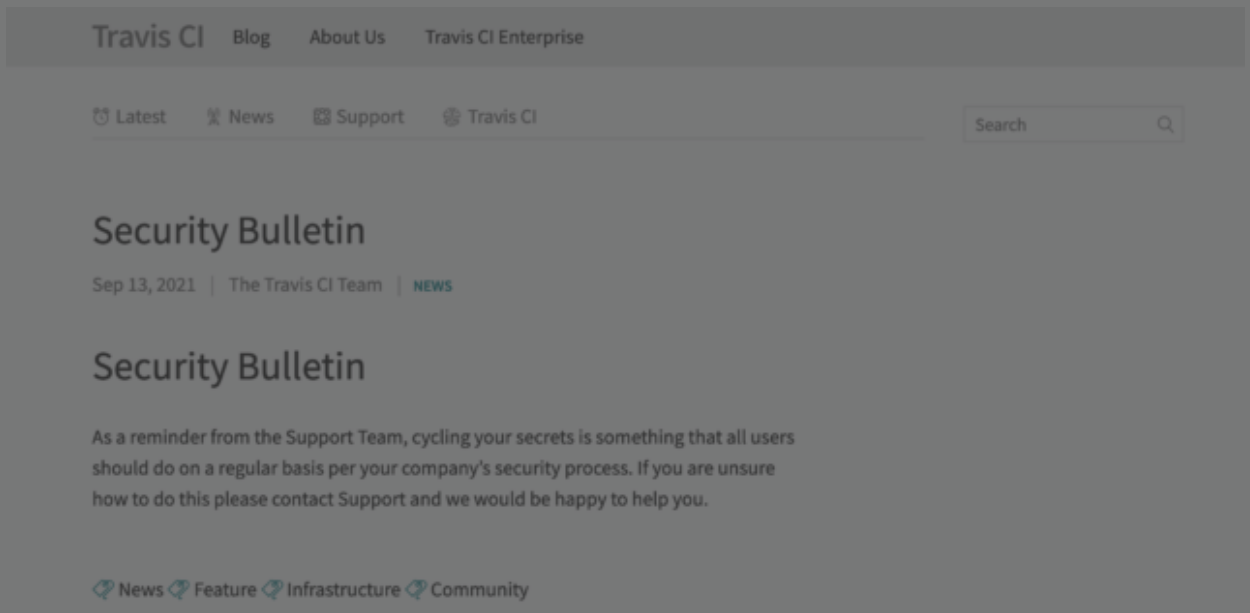
In a long Twitter thread, Péter Szilágyi details the arduous process that his group endured as it waited for Travis CI to take action and release a brief security bulletin on an obscure webpage.





"After 3 days of pre n the 10th. No analysis, no securit secrets might have been stolen,"

After Szilágyi and L nd vulnerability disclosure processe multiple projects, [they] pos even a single 'thank you.' [No] acknowledgment of responsible disclosure. Not even admitting the gravity of it all," said Szilágyi, while referring to the security bulletin—and especially its abridged version, which included barely any details.



Enlarge / Yes, that's a legit security bulletin.

Szilágyi was joined by several members of the community in criticizing the bulletin. Boston-based web developer Jake Jarvis called the disclosure an "insanely embarrassing 'security bulletin.'"

But Travis CI thinks rotating secrets is something developers should be doing anyway. "Travis CI implemented a series of security patches starting on Sept 3rd that resolves this issue," concluded Mendy on behalf of the Travis CI team. "As a reminder, cycling your secrets is something that all users should do on a regular basis. If you are unsure how to do this, please contact Support."

Ars has reached ou aiting their responses.

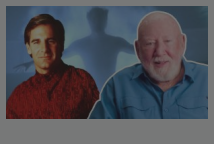
Update: 20:59 PT—a crets are not exposed from the "t nterface.

READER COMMENTS

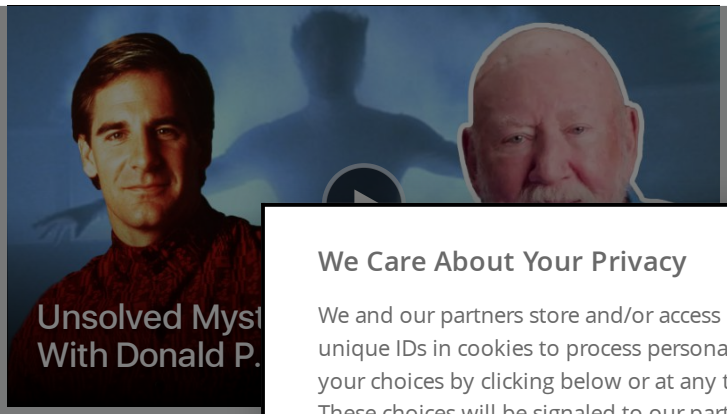
AX

Ax publications. His ex

CHANNEL ars

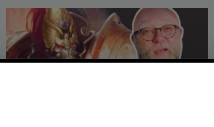


Unsolved Mysteries Of Quantum Leap



Today "Quantum Le
Bellisario joins Ars T
the lingering questi
popular show. Was
between all those ti
simply imagine it al
room do while Sam
to Sam's loyal ally A
finale, answers to th

With Donald P. Bellisario



Unsolved Mysteries
hammer
ith Author
nett

: F-16
ement search
l of F-35 fail?

Boeing 707

← PREVIOUS STORY

NEXT STORY →

Related Stories

Today on Ars

NEWSLETTER SIGNUP

Join the Ars Orbital Transmission mailing list to get weekly updates delivered to your inbox.

SIGN ME UP →