


Codecov hackers breached hundreds of restricted customer sites - sources

 [reuters.com/technology/codecov-hackers-breached-hundreds-restricted-customer-sites-sources-2021-04-19/](https://www.reuters.com/technology/codecov-hackers-breached-hundreds-restricted-customer-sites-sources-2021-04-19/)

Joseph Menn, Raphael Satter



Register now for FREE unlimited access to Reuters.com

SAN FRANCISCO, April 19 (Reuters) - Hackers who tampered with a software development tool from a company called Codecov used that program to gain restricted access to hundreds of networks belonging to the San Francisco firm's customers, investigators told Reuters.

Codecov makes software auditing tools that allow developers to see how thoroughly their own code is being tested, a process that can give the tool access to stored credentials for various internal software accounts.

The attackers used automation to rapidly copy those credentials and raid additional resources, the investigators said, expanding the breach beyond the initial disclosure by Codecov on Thursday. [read more](#)

Register now for FREE unlimited access to Reuters.com

The hackers put extra effort into using Codecov to get inside other makers of software development programs, as well as companies that themselves provide many customers with technology services, including IBM, one of the investigators said on condition of anonymity.

The person said both methods would allow the hackers to potentially gain credentials for thousands of other restricted systems.

IBM and other companies said that their code had not been altered, but did not address whether access credentials to their systems had been taken.

"We are investigating the reported Codecov incident and have thus far found no modifications of code involving clients or IBM," an IBM spokeswoman said.

The FBI's San Francisco office is investigating the compromises, and dozens of likely victims were notified on Monday. Private security companies were already beginning to respond to assist multiple clients, employees said.

Codecov did not respond to Reuters' request for comment on Monday.

Security experts involved in the case said the scale of the attack and the skills needed compared to last year's SolarWinds attack. The compromise of that company's widely used network management program led hackers inside nine U.S. government agencies and about 100 private companies.

It is unclear who is behind the latest breach or if they are working for a national government, as was the case with SolarWinds. [read more](#)

Others among Codecov's 19,000 customers, including big tech services provider Hewlett Packard Enterprise ([HPE.N](#)), said they were still trying to determine if they or their customers had been hurt.

"HPE has a dedicated team of professionals investigating this matter, and customers should rest assured we will keep them informed of any impacts and necessary remedies as soon as we know more," said HPE spokesman Adam Bauer.

Even Codecov users who had seen no evidence of hacking were taking the breach seriously, a corporate cybersecurity official told Reuters. He said his company was busy resetting its credentials and that his counterparts elsewhere were doing the same, as Codecov recommended.

Codecov earlier said hackers began tampering with its software on Jan. 31. It was only detected earlier this month when a customer raised concerns.

Codecov's website says its customers include consumer goods conglomerate Procter & Gamble Co, ([PG.N](#)) web hosting firm GoDaddy Inc, ([GDDY.N](#)) The Washington Post, and Australian software firm Atlassian Corporation PLC ([TEAM.O](#)). Atlassian said it had not yet seen any impact nor signs of a compromise.

The Department of Homeland Security's cybersecurity arm and the FBI declined to comment.

Register now for FREE unlimited access to Reuters.com

Reporting by Joseph Menn, Raphael Satter and Christopher Bing; Editing by Sam Holmes

Our Standards: [The Thomson Reuters Trust Principles.](#)