UPDATED 21:27 EST / DECEMBER 04 2019

SECURITY

Bug bounty startup HackerOne suffers breach after analyst mistake

BY DUNCAN RILEY

Bug bounty program startup HackerOne Inc. has suffered a security breach after accidentally giving a researcher the ability to read and modify some of its bug reports.

The incident occurred because an analyst at Hackerone who was corresponding with the researcher provided a cURL command that mistakenly included a valid session cookie. That gave anyone in possession the ability to access and modify the same data the analyst had access to.

First spotted today by Ars Technica, a researcher going by the
community board Nov. 24 that he had been given access and
did move quickly, revoking access to the session cookie two h
was made, but the question arises is how it occurred to begin

HackerOne's official explanation is that its security analyst fail
from a browser console that disclosed the session cookie.

cookies are tied to a particular application, in this case hackerone.com," HackerOne said. "The
n won't block access when a session cookie gets reused in another location. This was a known risk.

As many of HackerOne's users work from mobile connections and through proxies, blocking access would degrade the user experience for those users."

The company has now made changes to its security procedures. The researcher haxta4ok00 was also paid $20,000 for identifying and reporting the security issue.

"It is quite surprising that the security measures, now announced by HackerOne, were not implemented before, given that some of them are of a fundamental and indispensable nature," Ilia Kolochenko, founder and chief executive of web security company ImmuniWeb, told SiliconANGLE. Other corrective measures," he added, may also appear questionable, for example blocking access from specific countries.

"Security researchers may feel at least uncomfortable, if not embarrassed, in light of HackerOne's persistent advertising of diversified and international crowd intelligence," Kolochenko explained. "And importantly, sophisticated cybercriminals will bypass this 'measure' with the utmost of ease. Nonetheless, rapid and transparent disclosure of the incident by HackerOne serves as a laudable example to others and reminds us once again that humans are the weakest link."

Calling the announcement startling, Craig Young, computer security researcher for Tripwire Inc.'s vulnerability and exposure research team, noted that, similar to previously disclosed incidents or weaknesses within BugZilla or Google Issue Tracker, exposure of nonpublic HackerOne reports is a danger to all internet users.

"While I commend HackerOne for their response, this incident is yet another reminder of the distinct risk organizations take by using managed vulnerability reporting services like BugCrowd or HackerOne," Young added. "The consolidation of valuable data by such vendors creates a hugely attractive attack target for intelligence agencies or even criminal actors to fill their arsenal."

Photo: HackerOne

LATEST STORIES

Bug bounty startup HackerOne suffers breach after analyst mistake

SECURITY - BY DUNCAN RILEY . 2 HOURS AGO

CloudBees debuts Jenkins X as a service on Google Cloud

CLOUD - BY MIKE WHEATLEY . 3 HOURS AGO

Israeli cybersecurity startup Panorays raises $15M

SECURITY - BY DUNCAN RILEY . 3 HOURS AGO

TikTok's parent company taken to court for collecting data on children

APPS - BY JAMES FARRELL . 3 HOURS AGO

Canonical offers optimized Ubuntu Pro images on AWS

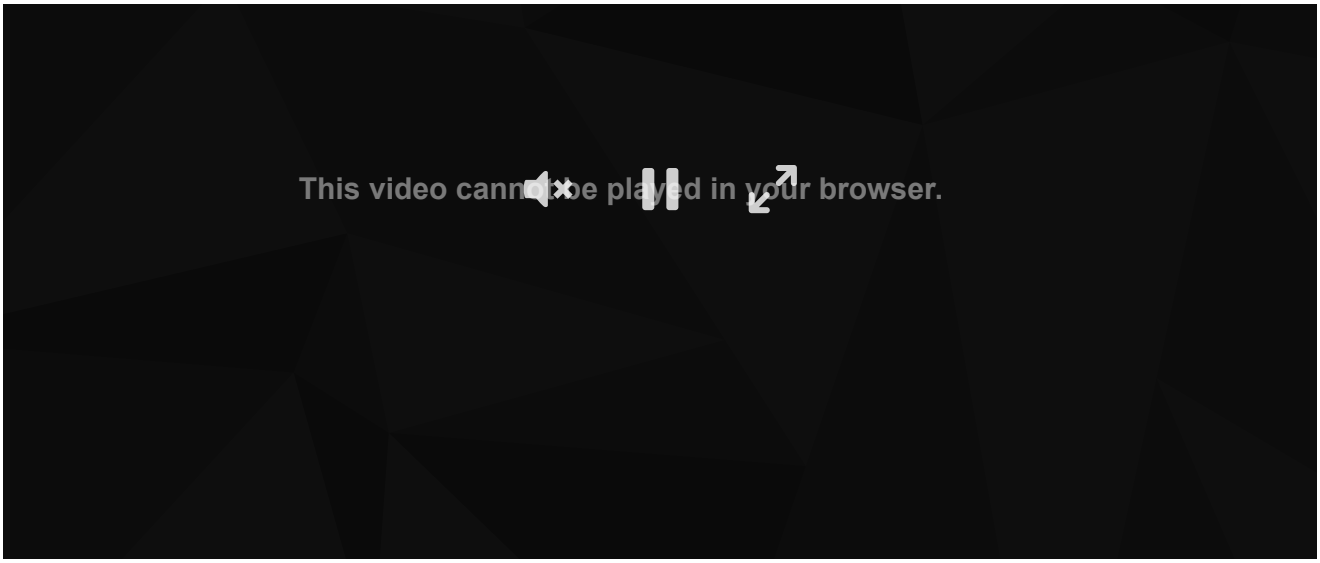
CLOUD - BY MIKE WHEATLEY . 4 HOURS AGO

Greylock investor rides waves of opportunity in wake left by large enterprise cloud players

CLOUD - BY MARK ALBERTSON . 8 HOURS AGO

CUBE EVENT COVERAGE

SHARE



Explore more videos at theCUBE

LATEST FROM THECUBE

VMware's partnership with AWS highlights delicate balance as it navigates hybrid world

Fight to finish: AI-on-AI and dev-on-dev speed up model training

Greylock investor rides waves of opportunity in wake left by large enterprise cloud players

Verizon and AWS get their game on, as 5G edge cloud computing goes live in Chicago

AI and digital tech have transformed the competitive landscape for many Accenture clients

Many throats to choke: For better or worse, multiple clouds are here to stay

CloudBees debuts Jenkins X as a service on Google Cloud

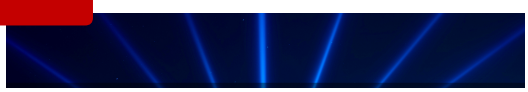
Exclusive: With new tech, Andy Jassy aims to take Amazon's cloud everywhere

Eirini 1.0 launch brings Kubernetes and Cloud Foundry closer together

At KubeCon, cloud-native starts to get real for the enterprise

View full report coverage

MING CUBE EVENTS



Cisco Live Barcelona 2020
Jan 27-31

Health Evolution Summit 2020
Apr 01-03

Red Hat Summit 2020
Apr 27-29

Dell Technologies World 2020
May 04-07

IBM Think 2020
May 04-07