Bug Bounty Programs Are Being Used to Buy Silence

Investigative report on how commercial bug-bounty programs like HackerOne, Bugcrowd, and SynAck are being used to silence researchers:

> Used properly, bug bounty platforms connect security researchers with organizations wanting extra scrutiny. In exchange for reporting a security flaw, the researcher receives payment (a bounty) as a thank you for doing the right thing. However, CSO's investigation shows that the bug bounty platforms have turned bug reporting and disclosure on its head, what multiple expert sources, including HackerOne's former chief policy officer, Katie Moussouris, call a "perversion."
>
> [...]
>
> Silence is the commodity the market appears to be demanding, and the bug bounty platforms have pivoted to sell what willing buyers want to pay for.
>
> "Bug bounties are best when transparent and open. The more you try to close them down and place NDAs on them, the less effective they are, the more they become about marketing rather than security," Robert Graham of Errata Security tells CSO.
>
> Leitschuh, the Zoom bug finder, agrees. "This is part of the problem with the bug bounty platforms as they are right now. They aren't holding companies to a 90-day disclosure deadline," he says. "A lot of these programs are structured on this idea of non-disclosure. What I end up feeling like is that they are trying to buy researcher silence."
>
> The bug bounty platforms' NDAs prohibit even mentioning the existence of a private bug bounty. Tweeting something like "Company

> X has a private bounty program over at Bugcrowd" would be enough to get a hacker kicked off their platform.
>
> The carrot for researcher silence is the money — bounties can range from a few hundred to tens of thousands of dollars — but the stick to enforce silence is "safe harbor," an organization's public promise not to sue or criminally prosecute a security researcher attempting to report a bug in good faith.

Tags: bribes, cover-ups, disclosure, reports

Posted on April 3, 2020 at 6:21 AM • 19 Comments

Subscribe to comments on this entry

← Marriott Was Hacked — Again Security and Privacy Implications of Zoom →

Sidebar photo of Bruce Schneier by Joe MacInnis.