Previous article Next article

Google Ups the Bug Bounty Ante to $3133.7

Author:
Dennis Fisher

July 20, 2010 / 10:47 pm

Share this article:

Just four days after Mozilla announced it was increasing the bounty paid for critical security bugs in its software to $3,000, Google has upped the ante, saying that it will now pay $3133.70 for the most severe bugs researchers find in Chromium.

Just four days after Mozilla announced it was increasing the bounty paid for critical security bugs in its software to $3,000, Google has upped the ante, saying that it will now pay $3133.70 for the most severe bugs researchers find in Chromium.

"The maximum reward for a single bug has been increased to **$3,133.7**. We will most likely use this amount for SecSeverity-Critical bugs in Chromium. The increased reward reflects the fact that the sandbox makes it harder to find bugs of this severity," Chris Evans, a Google security researcher, said in a blog post. "Whilst the base reward for less serious bugs remains at $500, the panel

v

The sudden change in the price paid for bugs by both Mozilla and Google can be seen as a consequence of the stance taken by some researchers who have said that they're no longer interested in doing the software vendors' security work for them without any monetary reward. Prominent researchers such as Alex Sotirov, Charlie Miller and Dino Dai Zovi have said in the last year that vendors shouldn't expect researchers to continue finding serious bugs in their software and then wading through what can be a long process from reporting to patching to disclosure.

At the CanSecWest conference in 2009, Miller, Sotirov and Dai Zovi announced their "no more free bugs" campaign, saying that there were plenty of legitimate buyers willing to pay tens of thousands of dollars for critical bugs, so it made no sense for researchers to continue to feed the vendors free bugs.

"I was shocked when I saw someone sign up to go after IE 8 [at CanSecWest]. You can get paid a lot more than $5,000 for one of those bugs. I've talked to a lot of smart, knowledgeable people and no one knows exactly how he did it. [Nils] could easily get $50,000 for that vulnerability. I'd say $50,000 is a low-end price point," Miller said in an interview at the time, referring to the contestants in the Pwn2Own contest at CanSecWest. "For the amount of time he spent to do what he did on IE and Firefox, he could have found and exploited five or 10 Safari bugs. With the way they're paying $5,000 for every verifiable bug, he could have spent that same time and resources and make $25,000 or $30,000 easily just by going after Safari on Mac."

The announcement from Google, coming so closely on the heels of the Mozilla decision, could increase the pressure on large vendors such as Apple, Adobe and Microsoft to pay bug bounties as well. Microsoft officials have consistently said in recent years that they have no plans to start paying for vulnerabilities, as has Adobe.

But the landscape seem to be shifting quickly these days, so one never knows. Google's Chromium bounty program began in January and the company said it considers the idea a success already.

"Although still early days, the program has been a clear success. We have been notified of numerous bugs, and some of the participants have made it clear that it was the reward program that motivated them to get involved with Chromium security," Evans wrote.

- Placing a disclosure deadline on any serious vulnerability they report, consistent with complexity of the fix. (For example, a design error needs more time to address than a simple memory corruption bug).

- Responding to a missed disclosure deadline or refusal to address the problem by publishing an analysis of the vulnerability, along with any suggested workarounds.

- Setting an aggressive disclosure deadline where there exists evidence that blackhats already have knowledge of a given bug.

The blog post also said that the company would be following the same rules itself for responding to vulnerability reports in Google products from outside researchers, acknowledging that the company hadn't always met its own goals for response in the past.

[block:block=47]

"We would invite other researchers to join us in using the proposed disclosure deadlines to drive faster security response efforts. Creating pressure towards more reasonably-timed fixes will result in smaller windows of opportunity for blackhats to abuse vulnerabilities. In our opinion, this small tweak to the rules of engagement will result in greater overall safety for users of the Internet," the researchers wrote.

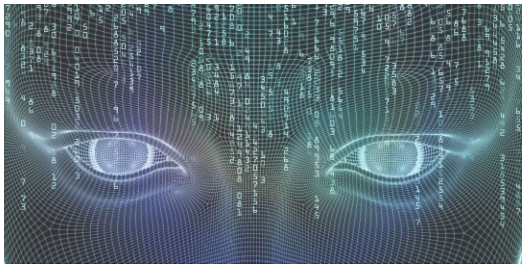
The disclosure post was credited to several of Google's top researchers, including Neel Mehta, Tavis Ormandy and Michal Zalewski.

Vulnerabilities Web Security

Google Warns of Critical Android Remote Code Execution Bug

Google's Android security update addressed 43 bugs overall affecting Android handsets, including Samsung phones.

January 5, 2021 2



Researcher Breaks reCAPTCHA With Google's Speech-to-Text API

Researcher uses an old unCAPTCHA trick against latest the audio version of reCAPTCHA, with a 97 percent success rate.

January 4, 2021 1

The 5 Most-Wa Threatpost Sto

A look back at what readers — offering a security stories that mind for security pr consumers through

December 30, 2020

INFOSEC INSIDER

Securing Your Move to the Hybrid Cloud

August 1, 2022

Why Physical Security Maintenance Should Never Be an Afterthought

July 25, 2022

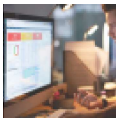
Conti's Reign of Chaos: Costa Rica in the Crosshairs

July 20, 2022

How War Impacts Cyber Insurance

July 12, 2022

Rethinking Vulnerability Management in a Heightened Threat Landscape



July 11, 2022

Follow @threatpost

The First Stop For Security News