Previous article Next article

Mozilla Bumps Bug Bounty to $3,000

Author:

Share this article:

In an effort to enlist more help finding bugs in its most popular software, such as Firefox, Thunderbird and Firefox Mobile, Mozilla is jacking up the bounty it pays to researchers who report security flaws to $3,000.

In an effort to enlist more help finding bugs in its most popular software, such as Firefox, Thunderbird and Firefox Mobile, Mozilla is jacking up the bounty it pays to researchers who report security flaws to $3,000.

The new price tag is a major increase over the payment of $500 with which the Mozilla Foundation launched its bug bounty program six years ago. Mozilla is one of a handful of vendors who make it known publicly that it will pay for bugs found in their software and reported directly to them. The foundation does set out quite a few conditions in order for a researcher to claim the payment, namely that the bug must be a critical security flaw and must be remotely exploitable.

Lucas Adamski, director of security engineering at Mozilla, said that the organization decided to increase its payments in reaction to the changes that have occurred in the security landscape since the program launched in 2004.

"For new bugs reported starting July 1st, 2010 UTC we are changing the bounty payment to $3,000 US per

eligible security bug. A lot has changed in the 6 years since the Mozilla program was announced, and we believe that one of the best way to keep our users safe is to make it economically sustainable for security researchers to do the right thing when disclosing information," Adamski wrote in a blog post. "We have also clarified the products covered under the bounty to better reflect the threats we are focused upon. We still include Firefox and Thunderbird obviously, but we also added Firefox Mobile and any Mozilla services that those products rely upon for safe operation."

In order to be eligible for the $3,000 payment, a researcher must meet the following conditions with his bug, according to Mozilla:

- Security bug must be original and previously unreported.
- Security bug must be a remote exploit.
- Security bug is present in the most recent supported, beta or release candidate version of Firefox, Thunderbird, Firefox Mobile, or in Mozilla services which could compromise users of those products, as released by Mozilla Corporation or Mozilla Messaging.
- Security bugs in or caused by additional 3rd-party software (e.g. plugins, extensions) are excluded from the Bug Bounty program.

The increased bug bounty by Mozilla is a good indication of the direction things have been taking in the vulnerability research arena in the last couple of years. Since organizations such as TippingPoint's Zero Day Initiative and VeriSign's iDefense have begun buying vulnerabilities from researchers, establishing a legitimate public marketplace for bugs, there has been a steady increase in pressure from researchers on vendors to do the same and offer bug bounties.

In addition to Mozilla, Google also has established a bug bounty program. However, none of the larger software vendors such as Microsoft or Oracle have taken that step. Some researchers see that as an inevitiability, however.

[block:block=47]

"Everyone can agree there's still room for improvement on third parties discovering vulnerabilities. It's correct that independent researchers need something more than a one-line acknowledgement. That's not enough for them to spend four months on a vulnerability, then have to prove it to the vendor and do a lot of the work for them. What Microsoft and others are concerned about is it turning into a ransom situation, but I don't see that," Marc Maiffret, CTO of eEye Digital Security said in a recent interview with Threatpost. "This is an important thing. There's not enough dialogue between the researchers and Microsoft or other vendors. They're not

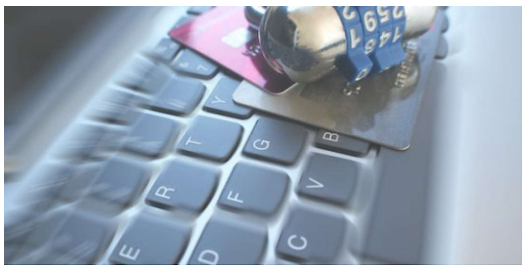
really talking. It's just as much Microsoft as the researchers. The researchers never say what Microsoft can do to make them happy. That hasn't happened yet. It's crucial because there was a significant number of guys responsibly reporting to Microsoft. And now they're not because they're being sold to defense contractors or underground buyers or whatever."

One other detail of the Mozilla bug bounty program: Researchers who report a bug also get a Mozilla t-shirt. Which is nice.

Share this article:

Web Security

SUGGESTED ARTICLES



Years-Long 'SilentFade' Attack Drained Facebook Victims of $4M

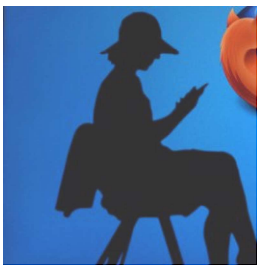
Facebook detailed an ad-fraud cyberattack that's been ongoing since 2016, stealing Facebook credentials and browser cookies.

October 2, 2020

Why Web Browser Padlocks Shouldn't Be Trusted

Popular 'safe browsing' padlocks are now passe as a majority of bad guys also use them.

September 29, 2020 3



Firefox 81 Relea Severity Code-

Mozilla has fixed thr flaws with the releas Firefox ESR 78.3.

September 22, 2020

DISCUSSION

INFOSEC INSIDER

You Can't Eliminate Cyberattacks, So Focus on Reducing the Blast Radius

May 12, 2022

CANs Reinvent LANs for an All-Local World

May 5, 2022 1

Bad Actors Are Maximizing Remote Everything

May 2, 2022

Skeletons in the Closet: Security 101 Takes a Backseat to 0-days

April 22, 2022

The Uncertain Future of IT Automation

March 8, 2022 2