Previous article Next article

Microsoft Says No to Paying Bug Bounties

Author:
Dennis Fisher

July 22, 2010 / 8:54 pm

Microsoft has no plans to follow in the footsteps of Mozilla and Google and pay researchers cash rewards for the bugs that they find in Microsoft's products.

Microsoft has no plans to follow in the footsteps of Mozilla and Google and pay researchers cash rewards for the bugs that they find in Microsoft's products.

In the wake of both Mozilla and Google significantly increasing their bug bounties to the $3,000 range, there have been persistent rumors in the security community that Microsoft soon would follow suit and start paying bounties as well. However, a company official said on Thursday that Microsoft was not interested in paying bounties.

"We value the researcher ecosystem, and show that in a variety of ways, but we don't think paying a per-vuln bounty is the best way. Especially when across the researcher community the motivations aren't always financial. It is well-known that we acknowledge researcher's contributions in our bulletins when a researcher has coordinated the release of vulnerability details with the release of a security update," Microsoft's Jerry Bryant said in an email. "While we do not provide a monetary reward on a per-bug basis, like any other industry, we do recognize and honor talent. We've had several influential folks from the researcher community join our security teams as Microsoft employees. We've also entered into contracts directly with many vendors and sometimes individual researchers to test our products for vulnerabilities before they're released. Many of these vendors and individuals first came to our attention based on the high-quality and unique approaches demonstrated by the vulnerabilities they reported to the MSRC."

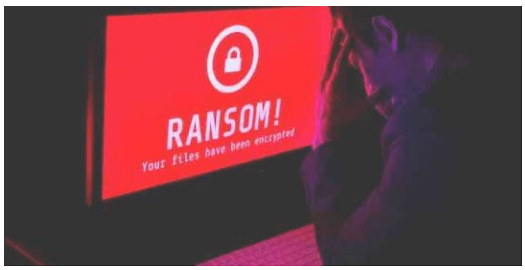
Some researchers have been calling on large software vendors such as Microsoft, Adobe, Apple and others to pay for the bugs that outsiders find in their products, but so far none of these companies has shown any indication that they're willing to do so. Third-party vulnerability buyers such as TippingPoint's Zero Day Initiative and iDefense Labs pay varying amounts for vulnerabilities, depending upon the severity of the bug. And there is also an unknown number of bugs sold to government agencies, defense contractors and other buyers in private sales every year.

Mozilla last week said it was raising its bug bounty to $3,000, and Google made a similar move four days later, jacking its top price up to $3,133.7.

[block:block=47]

Microsoft has been using outside researchers to test their software for security flaws on a contract and one-off basis for years now. But much of that work goes to boutique consultancies and not to individual researchers who find the bugs on their own time. That's one of the reasons that some researchers have been encouraging their peers to stop reporting vulnerabilities to vendors who don't pay bug bounties. The reasoning being that the vendors have their own in-house testers and consultants, who are getting paid, so there's nothing in it for outside researchers, aside from an acknowledgement from the vendor.

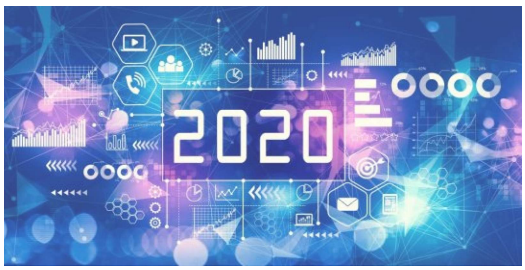
Vulnerabilities



New Year, New Ransomware: Babuk Locker Targets Large Corporations

Despite being a mostly run-of-the-mill ransomware strain, Babuk Locker's encryption mechanisms and abuse of Windows Restart Manager sets it apart.

January 7, 2021



The 5 Most-Wanted Threatpost Stories of 2020

A look back at what was hot with readers — offering a snapshot of the security stories that were most top-of-mind for security professionals and consumers throughout the year.

December 30, 2020

Tech Giants Le Support in Spy Against NSO G

Google, Microsoft, others want appeals immunity to Israeli alleged distribution illegal cyber-surveill

December 22, 2020

DISCUSSION

Anonymouse on December 10, 2010

It takes lots of time and effort to find unreported vulnerabilities, yet researchers are not being compensated for their work... Why should researchers bother reporting these bugs privately to companies first? Why reward the company when they will not reward the researcher? What should then motivate the researcher to continue discovering software flaws so that software for all of us is more secure? I'm sorry but handing out, "A for effort" and building up your "e-cred" without a financial return offers little incentive to work with companies.

-mouse

INFOSEC INSIDER

The Uncertain Future of IT Automation

March 8, 2022

6 Cyber-Defense Steps to Take Now to Protect Your Company

1

February 25, 2022

The Harsh Truths of Cybersecurity in 2022, Part II

2

February 24, 2022

3 Tips for Facing the Harsh Truths of Cybersecurity in 2022, Part I

February 9, 2022