Microsoft Security Response Center

Filling A Gap In the Vulnerability Market – First Bounty Notification

BlueHat / By bluehat / July 10, 2013 / BlueHat Prize, Bounty, bountyprograms, Internet Explorer (IE), Microsoft Windows, Responsible Disclosure, Security Research, Zero-Day Exploit

When Microsoft decided to offer not one but three new bounties, paying outside researchers directly for security research on some of our latest products, we put a lot of thought into developing those bounty programs. We developed a customized set of programs designed to create a win-win between the security researcher community and Microsoft's customers, by focusing on key data about what researchers were doing with vulnerabilities they found in our products. We monitored trends, and made the decision to jump into the vulnerability and exploit market in a specific, deliberate way.

I'd like to share some highlights of the programs thus far. I'll also expand on our strategic goals (and non-goals) for the programs, as they relate to the vulnerability and exploit marketplace.

So Far, Sooooo Good! The Data Supports Our Hypothesis

The security community has responded enthusiastically to our new bounty programs, submitting over a dozen issues for us to investigate in just the first two weeks since the programs opened. I personally notified the very first bounty recipient via email today that his submission for the Internet Explorer 11 Preview Bug Bounty is confirmed and validated. (Translation: He's getting paid.)

We have other researchers who have qualified for bounties under the IE11 program as well, and their notifications will be coming from secure [at] Microsoft [dot] com this week and beyond. We plan to add an acknowledgement page on our bounty web site, listing the researchers who would like to be publicly recognized for their contributions to helping us make our products more secure, so look for that page to appear linked from www.microsoft.com/bountyprograms in the near future.

Some key results we can share thus far, based on the data we have just two weeks into the new bounty programs:

- **More Submissions, Earlier** – We received more vulnerability reports in the two weeks of the bounty programs than we normally would during an average month. This data shows that our strategy for getting more vulnerability reports earlier in the release cycle is working.
- **Attracting New Researchers** – Researchers who have rarely if ever reported directly to Microsoft before our bounty programs are now choosing to talk directly to us. This data shows that our strategy for attracting security researchers we normally wouldn't hear from directly is working.

Mind the Gap – It's Not about Being the Highest Bidder

Vulnerabilities and exploits affecting many vendors' products have been trafficked for years in the white, grey, and black markets. For us, the distinction in the markets hinges on the intended use of the vulnerability or exploit that is purchased. There is also a price difference, generally speaking, with significantly higher prices often paid on the black market.

Our goal was not to directly compete with the black (or even grey) market. Rather, our goal was to attract those researchers who are currently willing to sell in the white market, and get them to come forward directly to us a lot earlier.

To us, the "white market" means that the buyers typically purchase the information for defensive use. The buyers in this category are typically either the affected vendor itself (via bounty programs), or a white-market vulnerability broker who uses the information for their protection services or threat reports.

Three years ago we examined data concerning what those researchers who like to get vulnerabilities fixed were doing when they found vulnerabilities in Microsoft products. Back then, most of them were still choosing to come directly to us, even though white market brokers were already offering cash. That trend has changed over the past couple of years: more vulnerabilities are being held back by the researchers waiting for the various markets to start paying, typically after our code is released to manufacturing (RTM).

Note that the data may be very different for other vendors' products. Each vendor should do their own analysis on their vulns and how they are traded in the various existing markets to determine for themselves if a bounty program is right for their products and their customers.

The following graphic shows the gap in the existing vulnerability and exploit market that our new bounty programs are filling. Note that our deepest security investments are still in the pre-release stages, with the Security Development Lifecycle (SDL) helping to reduce or eliminate security issues before code is released even for preview. (You can't pen-test or bounty your way to security, so having a robust Security Development Lifecycle is the key to long term improvements in the overall security of any vendor's products.)

It's not about offering the most money, but rather about putting attractive bounties out at times where there are few buyers (if any). For our products, that tends to be during the preview (or beta) period.

Trying to be the highest bidder is a checkers move, and we're playing chess. Stay tuned for more announcements coming soon regarding other moves we're making in the realm of industry collaboration to help protect customers. In the meantime, we're looking forward to more high-quality submissions to our bounty programs, and we'll share more data on how the programs are working out as we go.

Hope to see you in Las Vegas at Black Hat in just a few weeks, where we will be doing LIVE judging of Mitigation Bypass Bounty submissions at our booth on July 31 and August 1, noonish.

Katie Moussouris
Senior Security Strategist, MSRC
https://twitter.com/k8em0 (that's a zero)

← Previous Post Next Post →

Search …

Categories

BlueHat (182)

Japan Security Team (977)

MSRC (1,020)

Security Research & Defense (374)

Tags

advisory (60) ANS (47) Attack (45) Attack Vector (68) Black Hat (33) BlueHat Security Briefings (55) Community-based Defense (99) Defense-in-depth (39) EcoStrat (34) EMET (68) Exploitability (77) Internet Explorer (IE) (156) malware (59) Microsoft Office (81) Microsoft Windows (106) Mitigations (128) monthly bulletin release (48) rating (48) Risk Assesment (104) security (82) Security Advisory (134) Security Bulletin (133) security bulletin release (44) Security Bulletins (39) Security Conference Engagement (56) Security Ecosystem (52) Security Engineering (42) Security Research (82) Security Update (140) Security Update Webcast (46) Security Update Webcast Q & A (70) Update Tuesday (63) Webcast (37) Windows Update (68) Workarounds (74) Zero-Day Exploit (36) アドバイザリ (160) セキュリティ (54) セキュリティ情報 (463) セキュリティ更新 (90) ワンポイント (39) 啓発 (45) 展開 (45) 時事ネタ (42) 脆弱性 (248)

Recent Posts

Publishing CBL-Mariner CVEs on the Security Update Guide CVRF API

Security Update Guide Improvement – Representing Hotpatch Updates

BlueHat 2023: Applications to Attend NOW OPEN!

A Ride on the Wild Side with Hacking Heavyweight Sick Codes

Announcing the Microsoft Machine Learning Membership Inference Competition (MICO)

Archives

Select Month