Microsoft Security Response Center

Heart of Blue Gold – Announcing New Bounty Programs

BlueHat / By bluehat / June 19, 2013 / BlueHat Prize, Bounty, bountyprograms, Mitigations, Security Ecosystem

Our Philosophy

At the heart of our community outreach programs, we've always had the same philosophy: help increase the win-win between Microsoft's customers and the security research community. We have evolved and deepened our relationships with this community since the earliest days of Microsoft's outreach. In the early 2000's, Microsoft had to go through what I call "the five stages of vulnerability response grief." This is a process that all vendors must invariably go through in order to reach the "Acceptance Stage," which includes working in a collaborative way, with security researchers and good old-fashioned hackers. We may not always have 100% philosophical alignment, but we always want to keep a dialog open with the research community to further the common goal of protecting customers.

This philosophy is reflected in a new strategy designed to increase protections through outreach in the security community. The new programs we are announcing today are critical components in delivering this strategy. Other programs focused on detection and protection will follow soon.

Today's new programs continue our focus of direct investments in the research community, calling upon the clever hackers of the world to work with us on strengthening our platform-wide defenses.

Our New Bounty Programs

Today is an inflection point for Microsoft, as well as the security industry. For the first time ever, Microsoft is offering direct cash payouts in exchange for reporting certain types of vulnerabilities and exploitation techniques. We are making this shift in order to learn about these issues earlier and to increase the win-win between Microsoft's customers and the security researcher community.

Full details for the new bounty programs and a fantastic technical deep-dive by our esteemed panel of judges (headed by Matt Miller and David Ross) can be found on SRD's blog.

In short, we are offering cash payouts for the following programs:

- **Mitigation Bypass Bounty** – Microsoft will pay up to $100,000 USD for truly novel exploitation techniques against protections built into the latest version of our operating system (Windows 8.1 Preview). Learning about new

exploitation techniques earlier helps Microsoft improve security by leaps, instead of one vulnerability at a time. This is an ongoing program and not tied to any event or contest.

- **BlueHat Bonus for Defense** – Microsoft will pay up to $50,000 USD for defensive ideas that accompany a qualifying Mitigation Bypass Bounty submission. Doing so highlights our continued support of defense and provides a way for the research community to help protect over a billion computer systems worldwide from vulnerabilities that may not have even been discovered.
- **IE11 Preview Bug Bounty** – Microsoft will pay up to $11,000 USD for critical vulnerabilities that affect IE 11 Preview on Windows 8.1 Preview. The entry period for this program will be the first 30 days of the IE 11 Preview period. Learning about critical vulnerabilities in IE as early as possible during the public preview will help Microsoft deliver the most secure version of IE to our customers.

The Mitigation Bypass Bounty and the BlueHat Bonus for defense are designed to operate together and to focus on our latest version of the Windows platform. Our platform-wide mitigations (DEP, ASLR, and so forth) are part of "the shield" that increases costs to attackers by making it difficult to reliably exploit individual vulnerabilities. Annual exploit competitions, like pwn2own, have been one way that Microsoft and other vendors have learned about these new techniques. We decided that we didn't want to wait for the next competition to learn about more of these new exploitation techniques – we want to know about them before they are used to target our customers. For Microsoft, learning about mitigation bypasses on our latest platform, or "holes in the shield," helps us better protect against entire classes of attacks and can help us move the state of security in our products by leaps, rather than by small increments that a traditional bug bounty alone would.

Why is the IE 11 Preview bug bounty only open for 30 days? Because we felt we could fill a gap in the vulnerability marketplace to the benefit of researchers, Microsoft engineers and our customers. While we work closely with white market vulnerability brokers like HP's Tipping Point Zero Day Initiative and iDEFENSE's Vulnerability Contributor Program, many of these organizations don't offer bounties for software in beta, so some researchers would hold onto vulnerabilities until the code is released to manufacturing. Learning about these vulnerabilities earlier is always better for us and for our customers.

The IE 11 Preview Bug Bounty is a way for Microsoft to provide incentives for the researcher community to come forward with their vulnerability reports directly and privately to us. The timing for our IE 11 Preview Bug Bounty allows for the vulnerability reports to arrive before the software is widely deployed by customers.

Together, the new bounty programs are designed to work collectively to encourage the security research community to report vulnerabilities in the latest browser and exploitation techniques across the latest platform to Microsoft as early as possible.

Our Future

While we're not the first vendors to enter the exploit and vulnerability market, we do expect that the landscape for our products and customers will shift as the ecosystem adjusts to this new approach. We'll be running these new bounty programs, learning and adjusting, much like other vendors who have waded in to the vulnerability marketplace before us. We'll announce the evolution of these programs as we develop them further and will share some of the highlights as we go.

From Microsoft's early days of outreach; days of throwing Black Hat's first big researcher appreciation party; to inviting hackers to Redmond for the first BlueHat conference in 2005; to hiring security researchers to pen test our products before release; to sponsoring or attending over 30 hacker conferences a year worldwide; to awarding more than $260,000 USD in cash and prizes to the three BlueHat Prize winners for defensive mitigation ideas–we have been investing in the research community in many ways. These new programs are an evolution of that investment.

One last note: It may not have escaped your notice that paying directly for vulnerability and exploit information is not the only way to work with an ecosystem to discover these kinds of issues. Stay tuned for more updates from our team in the coming weeks, especially in the realm of industry collaboration. With the strategic bounty programs announced today and the industry collaboration program enhancements to come, Microsoft will simultaneously encourage those who want to work with us while increasing costs for those whose actions cannot be affected by bounties or other incentive programs.

Our Thanks & gr33tz

Those who have worked on these programs know that it takes a village to raise a bounty —especially when it involves creating a new approach that is a true strategic shift. It's not something any one person can do alone and requires investment and thinking from many people. It's impossible to include everyone involved, but these are the folks I could grab for a photo, plus a couple photobombs from friends…Thanks for your help, past, present, and future. Together, we are miners for hearts of Blue Gold.

L-R: David Seidman, Gerardo di Giacomo, Mark Oram (via avatar), Mike Reavey, Dustin Childs, Leah Lease, Rob Chapman, Neil Sikka, Jacqueline Lodwig, Brandon Caldwell, Katie Moussouris, Nate Jones, Sweety Chauhan, Emily Anderson, Claudette Hatcher, Cynthia Sandwick, Stephen Finnegan, Manuel Caballero, Ben Richeson, Elias Bachaalany, David Ross, Cristian Craioveanu, Ken Johnson, Mario Heiderich, Jonathan Ness. Not pictured: Christine Aguirre, Danielle Alyias, Michal Chmielewski, Chengyun Chu, Jules Cohen, Bruce Dang, Jessica Dash, Richard van Eeden, Michelle Gayral, Cristin Goodwin, Angela Gunn, Joe Gura, Dean Hachamovitch, Chris Hale, Kyle Henderson, Forbes Higman, Andrew Howard, Kostya Kortchinsky, Jane Liles, Matt Miller, William Peteroy, Georgeo Pulikkathara, Rob Roberts, Matt Thomlinson, David Wheeler, Chris Williams. Behind the camera: Jerry Bryant.

Katie Moussouris
Senior Security Strategist, MSRC
on Twitter, @k8em0 (that's a zero)

← Previous Post Next Post →

Search ...

Categories

BlueHat (181)

Japan Security Team (945)

MSRC (979)

Security Research & Defense (371)

Tags

advisory (60) ANS (47) Attack (43) Attack Vector (68) Black Hat (33) BlueHat Security Briefings (55) Community-based Defense (92) Defense-in-depth (38) EcoStrat (34) EMET (68) Exploitability (77) Internet Explorer (IE) (156) malware (59) Microsoft Office (81) Microsoft Windows (106) Mitigations (126) monthly bulletin release (48) rating (48) Risk Asessment (104) security (79) 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 (78) Security Update (139) 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 (151) セキュリティ (54) セキュリティ情報 (458) セキュリティ更新 (83) ワンポイント (39) 啓発 (45) 展開 (45) 時事ネタ (42) 脆弱性 (246)

Recent Posts

Exploring a New Class of Kernel Exploit Primitive

Guidance for CVE-2022-23278 spoofing in Microsoft Defender for Endpoint

Disclosure of Vulnerability in Azure Automation Managed Identity Tokens

Cyber threat activity in Ukraine: analysis and resources

Researcher Spotlight: Cyber Viking Nate Warfield is Here to Help

Archives

Select Month