Microsoft Security Response Center

A Call for Better Coordinated Vulnerability Disclosure

MSRC / By msrc / January 11, 2015 / Coordinated Vulnerability Disclosure, CVD

For years our customers have been in the trenches against cyberattacks in an increasingly complex digital landscape. We've been there with you, as have others. And we aren't going anywhere. Forces often seek to undermine and disrupt technology and people, attempting to weaken the very devices and services people have come to depend on and trust. Just as malicious acts are planned, so too are counter-measures implemented by companies like Microsoft. These efforts aim to protect everyone against a broad spectrum of activity ranging from phishing scams that focus on socially engineered trickery, to sophisticated attacks by persistent and determined adversaries. (And yes, people have a role to play – strong passwords, good policies and practices, keeping current to the best of your ability, detection and response, etc. But we'll save those topics for another day).

With all that is going on, this is a time for security researchers and software companies to come together and not stand divided over important protection strategies, such as the disclosure of vulnerabilities and the remediation of them.

In terms of the software industry at large and each player's responsibility, we believe in Coordinated Vulnerability Disclosure(CVD). This is a topic that the security technology profession has debated for years. Ultimately, vulnerability collaboration between researchers and vendors is about limiting the field of opportunity so customers and their data are better protected against cyberattacks.

Those in favor of full, public disclosure believe that this method pushes software vendors to fix vulnerabilities more quickly and makes customers develop and take actions to protect themselves. We disagree. Releasing information absent context or a stated path to further protections, unduly pressures an already complicated technical environment. It is necessary to fully assess the potential vulnerability, design and evaluate against the broader threat landscape, and issue a "fix" before it is disclosed to the public, including those who would use the vulnerability to orchestrate an attack. We are in this latter camp.

CVD philosophy and action is playing out today as one company – Google – has released information about a vulnerability in a Microsoft product, two days before our planned fix on our well known and coordinated Patch Tuesday cadence, despite our request that they avoid doing so. Specifically, we asked Google to work with us to protect customers by withholding details until Tuesday, January 13, when we will be releasing a fix. Although following through keeps to Google's announced timeline for disclosure, the decision feels less like principles and more like a "gotcha", with customers the ones who may suffer as a result. What's right for Google is not always right for customers. We urge Google to make protection of customers our collective primary goal.

Microsoft has long believed coordinated disclosure is the right approach and minimizes risk to customers. We believe those who fully disclose a vulnerability before a fix is broadly available are doing a disservice to millions of people and the systems they depend upon. Other companies and individuals believe that full disclosure is necessary because it forces customers to defend themselves, even though the vast majority take no action, being largely reliant on a software provider to release a security update. Even for those able to take preparatory steps, risk is significantly increased by publically announcing information that a cybercriminal could use to orchestrate an attack and assumes those that would take action are made aware of the issue. Of the vulnerabilities privately disclosed through coordinated disclosure practices and fixed each year by all software vendors, we have found that almost none are exploited before a "fix" has been provided to customers, and even after a "fix" is made publicly available only a very small amount are ever exploited. Conversely, the track record of vulnerabilities publicly disclosed before fixes are available for affected products is far worse, with cybercriminals more frequently orchestrating attacks against those who have not or cannot protect themselves.

Another aspect of the CVD debate has to do with timing – specifically the amount of time that is acceptable before a researcher broadly communicates the existence of a vulnerability. Opinion on this point varies widely. Our approach and one that we have advocated others adopt, is that researchers work with the vendor to deliver an update that protects customers prior to releasing details of the vulnerability. There are certainly cases where lack of response from a vendor(s) challenges that plan, but still the focus should be on protecting customers. You can see our values in action through our own security experts who find and report vulnerabilities in many companies' products, some of which we receive credit for, and many that are unrecognized publically. We don't believe it would be right to have our security researchers find vulnerabilities in competitors' products, apply pressure that a fix should take place in a certain timeframe, and then publically disclose information that could be used to exploit the vulnerability and attack customers before a fix is created.

Responding to security vulnerabilities can be a complex, extensive and time-consuming process. As a software vendor this is an area in which we have years of experience. Some of the complexity in the timing discussion is rooted in the variety of environments that we as security professionals must consider: real world impact in customer environments, the number of supported platforms the issue exists in, and the complexity of the fix. Vulnerabilities are not all made equal nor according to a well-defined measure. And, an update to an online service can have different complexity and dependencies than a fix to a software product, decade old software platform on which tens of thousands have built applications, or hardware devices. Thoughtful collaboration takes these attributes into account.

To arrive at a place where important security strategies protect customers, we must work together. We appreciate and recognize the positive collaboration, information sharing and results-orientation underway with many security players today. We ask that researchers privately disclose vulnerabilities to software providers, working with them until a fix is made available before sharing any details publically. It is in that partnership that customers benefit the most. Policies and approaches that limit or ignore that partnership do not benefit the researchers, the software vendors, or our customers. It is a zero sum game where all parties end up injured.

Let's face it, no software is perfect. It is, after all, made by human beings. Microsoft has a responsibility to work in our customers' best interest to address security concerns quickly, comprehensively, and in a manner that continues to enable the vast ecosystem that provides technology to positively impact peoples' lives. Software is organic, usage patterns and practices change, and new systems are built on top of products that test (and in some cases exceed) the limits of its original design. In many ways that's the exciting part of software within the rapidly evolving world that we live in. Stating these points isn't in any way an abdication of responsibility. It is our job to build the best possible software that we can, and to protect it continuously to the very best of our ability. We're all in.

Chris Betz
Senior Director, MSRC
Trustworthy Computing

[Note: In our own CVD policy (available at microsoft.com/cvd), we do mention exceptions for cases in which we might release an advisory about a vulnerability in a third party's software before an update is ready, including when the technical details have become publicly known, when there is evidence of exploitation of an unpatched vulnerability, and when the vendor fails to respond to requests for discussion.]

← Previous Post Next Post →

advisory (60) ANS (47) Attack (43) Attack Vector (68) Black Hat (33) BlueHat Security Briefings (55) Community-based Defense (93) Defense-in-depth (38) EcoStrat (34) EMET (68) Exploitability (77) Internet Explorer (IE) (156) malware (59) Microsoft Office (81) Microsoft Windows (106) Mitigations (127) monthly bulletin release (48) rating (48) Risk Asessment (104) security (80) 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 (79) 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

Archives

Select Month