Coordinated Vulnerability Disclosure: Bringing Balance to the Force

07/22/2010

Today on the MSRC blog, Matt Thomlinson, General Manager of Trustworthy Computing Security, announced our new philosophy on Coordinated Vulnerability Disclosure. I wanted to provide some context and history on how this came about. This post is about changing the way we at Microsoft talk about some familiar disclosure concepts, and is meant as an introduction to how Microsoft would like to engage with researchers. We're opening up a dialogue with the community here, and we welcome your feedback.

Responsible Disclosure (RD), Full Disclosure (FD) -- everybody has an opinion, and each believes that their way is the best way to keep users safe. For background, one general definition of RD as most vendors define it is that the issue is reported privately to the vendor *and no one else* until the vendor issues a patch. In contrast, proponents of FD provide all vulnerability details to everyone at the same time, a move designed to make vendors provide updates faster.

Needless to say, most vendors including Microsoft are in favor of RD, while finders fall across the spectrum from FD to RD. Ultimately, we are all part of a virtual security team with the common goal of making the Internet safer and protecting the people using it – it's good to remind everyone that we're on the same team, and we should keep the dialogue open, even when we disagree.

The term Coordinated Vulnerability Disclosure was first introduced to me by Jake Kouns of OpenSecurityFoundation.org, when we spoke at great length after I was on a panel at RSA on Responsible Disclosure. WeldPond (AKA Chris Wysopal, CTO of Veracode) recently tweeted: *“We need to start calling working with the vendor ‘Coordinated Disclosure.’ I agree that "Responsible" is too loaded.”*

The concept of making the name more descriptive makes perfect sense to me, since the term “responsible” can be subjective to so many. Even the ISO draft standard that was originally titled “Responsible Vulnerability Disclosure” is now called “Vulnerability Disclosure,” signaling that researchers, vendors, and (gasp!) even policy makers agree that the old term is more subjective.

The intention of RD was that it was designed to be a fair way to negotiate between researchers and vendors around vulnerability reporting and resolution. However, that has resulted in much debate, between vendors and finders. So, how do we move past this debate towards providing a better solution?

Responsible Disclosure should be deprecated in favor of something focused on getting the job done, which is to improve security and to protect users and systems. As such, Microsoft is asking researchers to work with us under Coordinated Vulnerability Disclosure, and added some coordinated public disclosure possibilities before a vendor-supplied patch is available when active attacks are underway. It uses the trigger of attacks in the wild to switch modes, which is an event that is objectively observable by many independent sources.

Make no mistake about it, CVD is basically founded on the initial premise of Responsible Disclosure, but with a coordinated public disclosure strategy if attacks begin in the wild. That said, what’s critical in the reframing is the heightened role coordination and shared responsibility play in the nature and accepted practice of vulnerability disclosure. This is imperative to understand amidst a changing threat landscape, where we all accept that no longer can one individual, company or technology solve the online crime challenge.

Here are the simple tenets of Coordinated Vulnerability Disclosure as we envision them.

Step 1: Keep it Private, Keep it Safe

? Reporting: Report the issue to the vendor, or to a CERT-CC or some other coordinator you trust who will report to the vendor privately, or sell it to a service that will.

? Communication and timelines: Under CVD, just the same as in RD, finders and vendors should try to agree to a timeframe for fixing the issue. Complex cases may take longer to fix, and Microsoft will be as transparent about our investigation with finders as we can be, to let them know where we are in the investigation and resolution process. We appreciate finders being flexible when we share information with them about why a fix may take longer than the finder thinks it should.

? Status updates: Also as in traditional Responsible Disclosure, under CVD Microsoft will provide timely updates and target dates for resolution so that a finder is aware of the case status.

? Alternative to FD when a vendor is not responding at all: In some circumstances, a vendor may be unwilling or unable to respond to a vulnerability report, which is what advance security advisories are for – advisories published with limited details and no Proof of Concept, plus mitigations and workarounds. Finders can try that before resorting to publishing full details if they can. Some vulns won’t lend themselves easily to this method, but the point is to try.

Step 2: Hurry Up and Wait

Vendors and many finders know there has to be a balance between speed and quality. For Microsoft, even a 1% test failure rate could affect millions of our customers, so we take testing for functionality impact as seriously as we do the testing to make sure the update comprehensively addresses the vulnerability.

Ideally, both vendors and finders should work diligently to find a solution that will keep customers safe. If finders are only interested in working on the attack, that's ok too, as long as they give the vendor a chance to do their investigation, engineering and testing.

Working together on the update, sharing ideas, and testing each other's ideas is sensible.

- It's great when a researcher offers their ideas on how the issue could be mitigated or even fully fixed, but vendors are in the best position to do the integration testing and application compatibility testing required, since they know their products and the full testing matrix that their customers require.
- When we have good relationships with finders, Microsoft will often offer our proposed solution to the finder to see if it comprehensively addresses the vulnerability from a security standpoint.
- If finders choose to, we would like to offer them a chance to share their proposed fixes with us if they want us to test against both security and application compatibility with our other products, or products typically found on our customers' machines.
    - The security testing for simple vulnerability classes like buffer overflows is typically very fast. More complex attacks, that rely on a multistep exploitation process, or vulnerabilities with multiple vectors to reach the vulnerable code require more security testing time. If security testing was all vendors had to do, we wouldn't have as many timing disagreements.
    - The other testing time will vary depending on the complexity of the functionality touched by the update, how the product is used and how other products integrate with the affected product.

Step 3: Coordinated Public Disclosure

Coordinate public release happens, ideally, when the vendor releases the update. In the case of publicly verifiable active attacks, details may be released prior to an update being released, with emphasis on giving details to protection providers.

- If there are active attacks in the wild, the finder and vendor work together on the best interim solution.
- The vendor and finder agree on what action to tell users to take to protect themselves.

For finders who still believe that Full Disclosure is the best way to protect users, we respectfully disagree, but we still want to work with you if you're willing. We'd encourage folks who support FD to still contact us, as we can then attempt to coordinate release of information with protections that are available. Of course, we still don't think this is the best method, because the vast majority of customers will only be protected with an update – but we believe that even this level of coordination is definitely better than none at all.

For example, CVD is how we will now handle things when we're the finders. When Microsoft finders discover issues in third party products, they can use the Microsoft Vulnerability Research Program (MSVR) to report the issues to the vendor. If attacks start in the wild, we may potentially release vulnerability details through the Microsoft Active Protections Program (MAPP) to AV/IDS/IPS providers, or issue a third party killbit in the case of vulnerable Active X controls. We would in all cases coordinate with the affected vendor whenever possible.

So that is Coordinated Vulnerability Disclosure in a nutshell - a renaming of Responsible Disclosure that provides expectations and a process for Microsoft and researchers to work together without either party clouding the discussion with a term that is easily misinterpreted, even in cases where disclosure philosophies may not be entirely in sync. We even want to work with Full Disclosure proponents whenever possible to arm protection providers ahead of attackers.

Not all roles in disclosure have been covered here, so stay tuned for more as we gather feedback from the community. I would like to thank the following people and organizations for their review on this concept, and I welcome further comments on this by the community, including researchers, vendors, coordinators, and users.   -Katie Moussouris

Jake Kouns, Open Security Foundation

Steve Christey, CVE Editor, MITRE

Avishai Avivi, Juniper Networks

Bruce Monroe, Intel PSIRT

Pete Allor

Toshio Miyachi, JPCERT Coordination Center

Brian Martin, Tenable Network Security

Art Manion, CERT Coordination Center

Damir Rajnovic (Gaus), Cisco

Dan Kaminsky, Chief Scientist, Recursion Ventures

Mike Caudill, Cisco PSIRT

Jeremiah Grossman, WhiteHat Security

Jayson Jean, iDefense-VeriSign

Ryan Permeh, McAffee

Cassio Goldschmidt, Symantec

Arturo ‘Buanzo’ Busleiman, Buanzo Consulting / ArCERT and ONTI Security Advisor

Andy Steingruebl, PayPal

Dino Dai Zovi, Independent Security Researcher, Trail of Bits

Chris Wysopal, CTO Veracode