Announcing Coordinated Vulnerability Disclosure

MSRC / By msrc / July 22, 2010

Today, Microsoft is announcing a shift in philosophy on how we approach the topic of vulnerability disclosure, reframing the practice of "Responsible Disclosure" to "Coordinated Vulnerability Disclosure." In recognition of the endless debate between responsible disclosure and full disclosure proponents and its ability to detract from meaningful and productive industry collaboration and customer defense, we believe that the community mindset needs to shift, framing a key point – that coordination and collaboration are required to resolve issues in a way that minimizes risk and disruption for customers.

Coordinated Vulnerability Disclosure (CVD): Newly discovered vulnerabilities in hardware, software, and services are disclosed directly to the vendors of the affected product, to a CERT-CC or other coordinator who will report to the vendor privately, or to a private service that will likewise report to the vendor privately. The finder allows the vendor an opportunity to diagnose and offer fully tested updates, workarounds, or other corrective measures before detailed vulnerability or exploit information is shared publicly. If attacks are underway in the wild, earlier public vulnerability details disclosure can occur with both the finder and vendor working together as closely as possible to provide consistent messaging and guidance to customers to protect themselves.

Responsibility is still imperative, but it is a shared responsibility across the community of security researchers, security product providers and other software vendors. Each member of this community of defenders plays a role in improving the overall security of the computing ecosystem.

CVD does not represent a huge departure from the current definition of

"responsible disclosure," and we would still view vulnerability details being released broadly outside these guidelines as putting customers at unnecessary levels of risk. However, CVD does allow for more focused coordination on how issues are addressed publicly. CVD's core principles are simple: vendors and finders need to work closely toward a resolution; extensive efforts should be made to make a timely response; and only in the event of active attacks is public disclosure, focused on mitigations and workarounds, likely the best course of action — and even then it should be coordinated as closely as possible.

As Microsoft shifts its philosophy to this new approach, we are asking the broader security community to embrace the purpose of this shift, which is ultimately about minimizing customer risk-not amplifying it. This distinction is critical. We recognize it's possible that very limited attacks may be happening without our knowledge. However, we fundamentally believe (and our experience over the last 10 years has shown) that once vulnerability details are released publicly, the probability of exploitation rises significantly. Without coordination in place to provide a security update or tested workarounds, risk to customers is greatly amplified.

It is evident from listening to those on both extremes of the disclosure argument that there is one thing that we are all trying to do: protect customers. We've been working with the security community closely for years to coordinate our actions for the benefit of customers. Coordinated vulnerability disclosure will help keep users safe.

For further perspective on CVD and how we see it working, please see Katie Moussouris' Ecostrat blog post at http://blogs.technet.com/b/ecostrat/archive/2010/07/22/coordinated-vulnerability-disclosure-bringing-balance-to-the-force.aspx.

Thank you,

Matt Thomlinson

General Manager, Trustworthy Computing Security