Threat Complexity Requires New Levels of Collaboration

07/27/2009 • 6 minutes to read

When complex security issues that affect multiple vendors arise, calling them “challenging” is an understatement. We created the Microsoft Vulnerability Research Program (MSVR) to meet those challenges, learn from those experiences and strengthen the ties of our community of defenders across the industry in the process. As the state of software security matures beyond straightforward issues such as buffer overflows and elevation of privilege, we are working diligently towards a new level of cross-industry collaboration on a scale never seen before. We must do so in order to provide our mutual customers with the best possible experience on our platform.

Handle:
StoneZ

IRL:
Adrian Stone

Rank:
Senior Security Program Manager Lead

Likes:
Predictive Analytics, Game Theory, Databases, Sports Cars, NFL Football, Direct People

Dislikes:
Losing, Liars, Posers, No Talent Clowns

Handle:

k8e

IRL:
Katie Moussouris

Rank:
Senior Security Program Manager

Likes:
Cool vulns (responsibly disclosed of course), girls with soldering irons, Spanish tapas, quantum teleportation

Dislikes:
Rudeness, socks-n-sandals, licorice

The recent Active Template Library (ATL) issue required us to find a new and more collaborative manner to respond to the developing threats as more information about the vulnerability details became public. MSVR was at the heart of the response and coordination, along with MSRC, to find a solution. As MSRC focused on what it does regularly, which is driving change within Microsoft, MSVR kicked into high gear to coordinate and assist as many third-party affected vendors as possible to help resolve an industry-wide issue.

Several firsts and questions had to be met head-on by our relatively young MSVR program now celebrating its first birthday.

· How do we maintain and respect the overarching tenets of Responsible Disclosure while sharing the issue outside of Microsoft?

· How do we communicate openly and directly with multiple impacted parties while not putting customers at risk by a potential broad disclosure prior to the availability of mitigation?

· How do we translate an issue that we came to understand very well to third parties that may not have the same technical history or security response methodologies and practices that we do?

· Can we coordinate across the industry so that everyone is moving to the same goal of addressing the problem, despite differing development practices and engineering requirement timelines?

The talented security researchers that reported the issue to Microsoft had done so in a responsible manner with the goal of improving the ecosystem and helping us protect our customers. At the same time, it became clear to us that this was an industry-wide problem and that the best way to secure the ecosystem was to notify affected vendors while engineering efforts were underway here in Redmond. Microsoft is a supporter of Responsible Disclosure, which aims to allow affected vendors to understand and try to resolve their respective issues before discussing the details of the issue publicly. In this instance, MSVR's actions demonstrated a variety of responsible disclosure recently dubbed "partial disclosure ," when we alerted third-party vendors who we believed had controls compiled with our vulnerable ATL headers. In the past year of MSVR operations, we have acted in the Responsible Disclosure roles of Finder and Coordinator. The ATL issue required us to act in both of those roles, plus in the role of affected Vendor.

While we knew we had to disclose technical details to a broad group, the clock was also ticking as we began to see more and more details about this issue being discussed and discovered in the security community. The original security researchers that reported the issue to us worked with us diligently and patiently to continue acting responsibly with their understanding of the problem, while we began developing a process and technical tools to analyze our controls and look for a solution. At the same time, we began the process of identifying and analyzing the controls that are most commonly deployed but were developed by other vendors. It is at this point we felt that we had a viable way to individually engage as many of these affected vendors as possible to discuss the impact of the issue as it relates to their potentially vulnerable controls.

Due to their potential scope, library-related vulnerabilities can often stir uncertainty and concern in the industry, so we focused our efforts to understand the true depth and breadth of the impact. Our analysis indicated that the vast majority of controls that would impact our users could be addressed by a few key vendors in the ecosystem. With this in mind, MSVR reached out to vendors who had the broadest footprint in the ecosystem that we believed were affected by the issue. We also felt confident that the defense-in-depth engineering solutions being worked on here at Microsoft would help provide a safeguard against attacks and allow other vendors more time to modify and recompile their own controls.

Overall, our goals and objectives were straightforward, if not exactly effortless, and required us to also leverage many of the key lessons learned by the MSRC over the years. After we distilled the actions and goals down to their most elemental levels, it became clear we had to move quickly on several fronts, including:

· Coming up with our own defense-in-depth solution to help protect customers and mitigate the threat.

· Taking steps to identify quickly the affected third-party vendors who we thought had the broadest impact on our platform.

· Finding the right security contacts at the vendors who met those criteria.

· Packaging and disseminating the vulnerability information to them securely.

Our goals in doing so were to:

· Alert as many of the community of vendors who have affected controls as possible that there was an issue with ATL.

· Provide the third-party vendors with technical details necessary to perform the broad analysis of all of their controls to look for the vulnerability in their products.

· Support the third-party vendors in their analysis, answering their questions, and clarifying the issue when necessary.

· Coordinate with the major affected third parties in both the release of the updates, as well as with guidance for our mutual customers.

We learned a lot during this process. After all, evolution requires change in the way we think and in the way we act, which leads to growth. We will incorporate these lessons into MSVR processes moving forward. We have formed stronger relationships across organizations that MSVR has worked with on other issues in the past, and we have forged many new bonds with security teams across company boundaries. Overall, we are very pleased with the positive industry response, and we salute our counterparts in the security organizations of all the third-party vendors we have worked with during this historic collaboration, including but not limited to Adobe and Sun. We are also incredibly thankful and appreciative of Ryan Smith and David Dewey, the original security researchers that reported the issue to us responsibly, as it was a multidimensional challenge that required significant patience and understanding on their part as we determined how to best address the problem.

As we move forward toward the next challenges on the security horizon, we can anticipate deeper integration among the community of defenders, whether they work for Microsoft or a third-party vendor, whether they are security researchers or are members of a CERT – we can expect more collaboration. After all, progress towards securing our platform, as has been made with our own SDL , will naturally lead to attacks being more complex, more dependent on how applications interact with each other and with the underlying operating system, and therefore will require us all to look past our company logos and focus on that threat horizon.

I'm Adrian Stone , who ran the ATL coordination and is the new driver of the MSVR program since July 1, and I'm Katie Moussouris, founder of the MSVR program, and together with the security community, we look forward to advancing community-based defense and helping to usher in this new age of collaborative security for the good of all our customers.