Coordinated Vulnerability Disclosure at Microsoft

Commentaire [1]: https://web.archive.org/web/20141201000000*/http://go.microsoft.com/?linkid=9770197

From the anounce here: https://msrc-blog.microsoft.com/2011/04/19/coordinated-vulnerability-disclosure-from-philosophy-to-practice/

Contents

Introduction

In July 2010, Microsoft announced a shift in philosophy on vulnerability disclosure, reframing its practice of Responsible Disclosure and moving to adopt Coordinated Vulnerability Disclosure as its new approach. The purpose of this shift was to move away from the endless and often unproductive debate between responsible and full disclosure proponents, and focus instead on the heightened role that coordination plays in minimizing risk to customers. Microsoft believes that the process of vulnerability disclosure is a shared responsibility best practiced in strong coordination between finders, vendors, and protection providers working together to protect customers, businesses, and critical infrastructure.

Microsoft's Approach to Coordinated Vulnerability Disclosure

Under the principle of Coordinated Vulnerability Disclosure, finders disclose newly discovered vulnerabilities in hardware, software, and services directly to the vendors of the affected product, to a national CERT 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 the opportunity to diagnose and offer fully tested updates, workarounds, or other corrective measures before any party discloses detailed vulnerability or exploit information to the public. The vendor continues to coordinate with the finder throughout the vulnerability investigation and provides the finder with updates on case progress. Upon release of an update, the vendor may recognize the finder in bulletins or advisories for finding and privately reporting the issue. If attacks are underway in the wild, and the vendor is still working on the update, then both the finder and vendor work together as closely as possible to provide early public vulnerability disclosure to protect customers. The aim is to provide timely and consistent guidance to customers to protect themselves.

Microsoft is 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. While Microsoft recognizes that limited attacks may be happening without our knowledge, we fundamentally believe that when vulnerability details are released publicly, the probability of exploitation rises significantly.

For related resources, visit Coordinated Vulnerability Disclosure.

Purpose of This Document

This document outlines Microsoft Corporation's (Microsoft) approach to Coordinated Vulnerability Disclosure (CVD) in three separate roles: finder, coordinator and vendor. Microsoft acts in the role of finder as a research organization finding and reporting security vulnerabilities to an affected third-party vendor. Microsoft acts in the role of coordinator when cooperatively informing multiple vendors of an issue that affects all of them and working toward a coordinated release of protection or remediation. Microsoft also works as a vendor, when vulnerabilities that affect Microsoft products and services are reported by external finders to be addressed by Microsoft.

This document aims to clarify how Microsoft communicates the disclosure of vulnerabilities with industry peers, customers, and the research community in a coordinated way. Lastly, this document explains how to engage with Microsoft in coordinated vulnerability disclosure, when Microsoft is acting in any of the three roles of finder, coordinator, and vendor.

While we have considered and documented the most common scenarios, some vulnerabilities may present unique scenarios and may require slight deviation from the processes outlined in this document. Microsoft endeavors to follow this approach with every scenario whenever possible.

Section 1. Microsoft as a Finder of Vulnerabilities

A. MSVR and the Reporting Process

Microsoft Vulnerability Research (MSVR) is responsible for the reporting and coordination of vulnerabilities that Microsoft employees find in non-Microsoft, third-party products and services that could impact the security of the Microsoft platform. This section outlines how MSVR handles reporting and coordinating third-party vulnerabilities. Note that for the purpose of this section the term "third-party" refers to the party who owns the vulnerable product or service and is able to address the issue via a patch, workaround, or other methods. In addition, we refer to the affected third parties as vendors for the purpose of this document.

Each phase of this process is described more fully below.

B. Vendor Vulnerability Documentation

This section outlines the documentation that MSVR creates for a given vulnerability that is reported to a vendor directly. This is for the purpose of providing the affected vendor with enough details to investigate and remediate the issue, and to provide awareness of what to expect, as well as consistency in reporting to vendors.

While the actual content of the vulnerability documentation will vary from issue to issue, the documentation includes the following elements:

- **MSVR Vulnerability Tracking Number.** An internal reference number for tracking of MSVR cases in the format, MSVR-yyyy-xxxx. For example, MSVR-2011-0231.
- **Vulnerability Summary.** An outline of the issue.
- **Test Environment.** The environment in which the vulnerability was observed. This includes the version of the vulnerable software or hardware, the version of the platform, and any special system configurations required for replicating the issue.
- **Technical Details.** The known technical details of the vulnerability.
- **Security Impact.** The security impact to systems affected by the vulnerability. MSVR uses the STRIDE threat model for categories of security impact: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.
- **Vulnerability Severity.** The MSVR evaluation of the severity of the vulnerability based on the same MSRC Security Bulletin Severity Rating System used to rate vulnerabilities in Microsoft software.
- **Crash Dump Information.** A crash dump, or pertinent portions of a crash dump, if the vulnerability causes the system to create one and if it relates to the investigation.
- **Proof of Concept and/or Exploit Code.** The proof of concept and/or exploit code, when available, that MSVR shares with vendors who require it in their testing. This is because in some cases, technical descriptions are not enough to help the vendor of the affected software to investigate the issue. Note that a single proof of concept exploit may identify only one potential vector to exploit the vulnerability. Therefore, vendors should perform their own root cause analysis to determine how to fix the underlying vulnerability comprehensively.
- **Root Cause Analysis.** The technical root cause of the vulnerability, when available, from MSVR's analysis.

This list is not exhaustive, nor is it intended to provide all types of information that MSVR may provide to a vendor as a part of a vulnerability report. It aims to provide a consistent, repeatable framework for sharing vulnerability information with vendors in order to facilitate coordination and remediation of the vulnerability.

C. MSVR to Vendor Communication

MSVR’s preferred communication method with the vendor is e-mail, using our address, msvr@microsoft.com. MSVR also prefers to use encrypted email but will not impose this requirement on a vendor that is unable to support encryption.

When complete, MSVR sends the vendor vulnerability information to the vendor's designated contact. Any vulnerability information provided to the vendor is not intended for public use, but for the vendor’s use to identify and remediate the vulnerability. Specifically, Microsoft opposes the public release of any exploit code, proof of concept, or any other technical details that aid in the creation of exploit code and amplify the potential risk to customers before the vendor can create, test, and release a comprehensive update, or before the vulnerability is being used in attacks.

While some vendors may have a standard, public e-mail address for the reporting of a vulnerability, others may not. MSVR will make reasonable efforts to contact the affected vendor to provide notice of the vulnerability. However, because we prefer using e-mail to report the vulnerability, in the absence of a standard or previously known address, MSVR will make reasonable efforts to perform the following:

- Contact the official domain administrative contacts for the vendor’s Web site
- Send e-mail to the following local-parts (the name@) in front of the vendor's domain name: security, secure, security-alert, secalert, support, psirt, info, or sales)
- Use alternate channels, such as through an existing Microsoft relationship
- Query search engines for e-mail addresses
- In extreme cases, contact an existing, mutual third-party relationship, which includes a vulnerability monitoring and reporting agency such as CERT.

In order to minimize the risk of vulnerability information being misdirected while attempting to identify the vendor contact, MSVR will not send the vulnerability report in the initial e-mail. The initial e-mail will be a simple introduction stating that we are attempting to identify the correct contact to report a vulnerability in the vendor’s products or services.

When the appropriate vendor contact is identified and confirms willingness to accept the vulnerability report, MSVR will provide the vulnerability report.

D. Affected Vendor Investigation and Remediation

When the vendor receives the vulnerability report, MSVR assumes that the vendor will begin investigating the issue. MSVR will in turn, to the best of its ability, answer any technical questions that the vendor may have.

During the investigation phase, MSVR periodically asks the affected vendor, via e-mail, for an update as to the progress of the investigation and a best estimate of a timeline to develop remediation. This enables MSVR to begin preparing the MSVR Advisory, discussed next, and ensure that work on the vulnerability continues to move forward.

In addition, upon vendor request and if MSVR has resources available, MSVR will strive to provide some testing and comments on the effectiveness of the planned remediation of the vulnerability. This can be particularly important because an ineffective remediation could introduce new vulnerabilities or foster regressions.

E. Coordinated Disclosure

An important and final step in the reporting process is alerting users of the affected product or service to the existence of the vulnerability, the associated risk, and the vendor-supplied remediation.

In coordination with the affected vendor, MSVR plans to release an MSVR Advisory, either at the same time or after the vendor releases its own advisory. The purpose of the MSVR Advisory is to alert those affected by the vulnerability and provide remediation details. Unlike the detailed vulnerability report sent to the affected vendor, the MSVR Advisory does not contain any technical details that can make it easier for attackers to exploit the vulnerability, but instead focuses on illustrating the risk and potential impact to users and on providing remediation steps to reduce or eliminate that risk.

If the vendor does not have an advisory process in place to alert users of the risk associated with the vulnerability and the available remediation, then the MSVR Advisory will provide guidance on how users of the product or service can protect themselves.

Under no circumstances will Microsoft release details of an unpatched vulnerability unless evidence of public attacks exists, as outlined in subsection F, Exceptions to the Vulnerability Public Disclosure Process, au-dessous. Even under these exceptions, Microsoft will attempt to coordinate with the affected vendor to provide guidance on how users can protect themselves. In the event of public attacks, Microsoft may also work with its partners to provide protection if a vendor-supplied remediation is not available.

An example of the content that could be included in an MSVR Advisory is Microsoft Security Advisory 953818, "Blended Threat from Combined Attack Using Apple's Safari on the Windows Platform."

F. Exceptions to the Vulnerability Public Disclosure Process

Unfortunately, sometimes a vulnerability becomes publicly known or is exploited before a vendor-supplied remediation is available. In this case, Microsoft makes reasonable efforts to coordinate with the affected vendor to release an MSVR Advisory that includes potential mitigations and workarounds. This provides users with information and possible actions to protect themselves against an active vulnerability until the vendor supplies their remediation.

Three main scenarios where MSVR may issue an MSVR Advisory prior to the vendor's release of its own remediation are as follows:

- **When vulnerability technical details have become publicly known.** If reasonable evidence that the vulnerability has become publicly known is found, then MSVR alerts the affected vendor to this fact and MSVR may issue an MSVR Advisory. Potential evidence of publicly known vulnerability details may include, but are not limited to, the following:

    - Technical details of the vulnerability are available to the general public via the Internet.
    - Disassembly or crash dump data with enough detail to either directly expose the vulnerability or provide enough details to infer the vulnerability are available to the general public via the Internet.
    - Proof of concept or exploit code leveraging the vulnerability is available on the Internet.

- **When evidence of exploitation of an unpatched vulnerability surfaces.** If reasonable evidence that the vulnerability is being exploited is found, then MSVR alerts the affected vendor to this change in the threat level and MSVR may issue an MSVR Advisory. Potential evidence of exploitation may include, but is not limited to, the following:

  - Malware exploiting the vulnerability is found on the Internet.
  - Targeted attacks that use the vulnerability via the Internet are either detected or reported.
  - Mass exploitation of the vulnerability via the Internet are either detected or reported.

- **When the vendor fails to respond.** Occasionally, the affected vendor does not respond to reasonable efforts to initiate contact or does not acknowledge the receipt of the vulnerability report. MSVR will then leverage existing contacts, business relationships, industry associations, or other connections with the vendor in order to help solicit a response. Only as a last resort, and after exhausting multiple various avenues and approaches for contact, will MSVR consider a vendor to be nonresponsive.

  If the vendor's vulnerability details become known publicly or if the vendor's unpatched vulnerability is exploited publicly, MSVR may issue an MSVR Advisory to provide users with notice of the vulnerability and potential mitigations or workarounds, if available. MSVR may also test new versions of the affected product or service for evidence of the vulnerability. If reasonable evidence that the vulnerability has been remediated is found, then the MSVR Advisory contains that information with the same non-technical detail as previously outlined, and directs users to the vendor's remediation.

Of course, in all cases, MSVR actively works to monitor the threat landscape and may work with partners to provide protections and mitigations for these issues. Microsoft's stated preference is to coordinate with vendors to remediate a vulnerability and protect users.

Section 2. Microsoft as a Vulnerability Coordinator

MSVR increasingly sees vulnerability researchers find more generic vulnerabilities or vulnerability classes that affect multiple vendors. Examples of these types of issues include a vulnerable, popular library used by multiple vendors, or a vulnerability in a protocol specification that has been implemented across multiple vendors. These issues typically require a level of coordination and management to minimize customer risk that many researchers simply do not have the time or resources to do. In addition, the fact that not every vendor has a consistent response to vulnerability reports, complicates matters further.

MSVR has unparalleled experience in dealing with these types of vulnerabilities to help minimize customer risk, and this section outlines how MSVR coordinates the reporting of vulnerabilities that affect multiple vendors. There are three typical scenarios in which MSVR becomes involved in multi-vendor vulnerability coordination:

- A Microsoft employee discovers a multi-vendor issue and reports it to MSVR for coordination.
- MSVR identifies a vulnerability or vulnerability class and coordinates its reporting.
- An external party reports a vulnerability to the Microsoft Security Response Center (MSRC) and either that external party or MSRC determines that the vulnerability impacts multiple vendors.

A. Vulnerability Reporting Process

The process in reporting a multi-vendor vulnerability does not typically deviate from what has been outlined in Section 1. Microsoft as a Finder of Vulnerabilities. However, some additional coordination is still required, as outlined in this subsection.

In the event that a vulnerability affects multiple vendors, MSVR follows the finder process set forth in Section 1; in particular, steps relevant to the particular vulnerability are as follows:

- Make reasonable efforts to identify every affected party and a confirmed point of contact at each.
- During the reporting phase, alert each vendor to the fact that this issue affects multiple other vendors such that a higher level of coordination may be required.
- If necessary, offer to host meetings with all affected vendors who wish to collaborate with the others in the investigation and remediation of the vulnerability.

In addition, if the vulnerability is reported by an external security researcher, MSVR performs the following:

- Communicate directly with the external security researcher and offer MSVR's assistance in coordinating with all affected vendors.
- Communicate any deadlines or other disclosure requirements that the external security researcher may have set with Microsoft or other affected vendors. While MSVR firmly believes that coordinated disclosure is the most effective way to handle a vulnerability, MSVR would rather have the chance to inform as many affected vendors as possible, even if the external security researcher does not share our disclosure philosophy.
- Communicate with all affected vendors and involved external security researchers the various scenarios under which MSVR may issue an MSVR Advisory before a vendor-supplied remediation is available, as documented in Section 1. Microsoft as a Finder of Vulnerabilities.
- Provide, where necessary and desired, introductions between the external security researcher and affected vendors in order to facilitate collaboration.
- Communicate any additional questions affected vendors may have to the external security researcher.

B. Coordinated Disclosure

While coordinated vulnerability disclosure is still the main goal in this scenario, MSVR understands that when multiple affected vendors are involved, not all vendors may be ready to release remediation at the same time. MSVR will communicate this possibility to all affected parties and everyone will be encouraged to share their investigation and remediation timelines, so that all affected parties can attempt to release around the same time. The stated goal is to coordinate response, remediation and disclosure as much as possible in order to minimize impact to end users and customers.

In addition, MSVR will draft and eventually release an MSVR Advisory alerting users to the issue but will not do so until all known affected vendors have released their remediation or if any of the previously outlined exceptions occur.

Section 3. Microsoft as an Affected Vendor

In the case where Microsoft is the vendor affected by a vulnerability, finders and coordinators submit vulnerability reports to Microsoft Security Response Center (MSRC) via secure@microsoft.com as outlined at the Microsoft Security Response Center Web site.

When MSRC receives the vulnerability report, a case manager provides an acknowledgement of the report to the sender and begins the triage process to determine the Microsoft product group to engage.

Being that the ultimate goal is to fix the vulnerability in a manner that reduces risk to users the most, the goals of MSRC are as follows:

- Assess the overall risk of the vulnerability report.
- Collaborate with the finder to understand and reproduce the vulnerability.
- Maintain communication with the finder on the progress of the case through the investigation, remediation, and testing process.
- Ensure that the finder understands Microsoft's position on Coordinated Vulnerability Disclosure.
- Facilitate communications, as required, between the finder and the necessary internal Microsoft product and services teams.
- Ensure that the finder, upon working in a coordinated manner with Microsoft, receives proper credit for reporting and collaboration.

Note that in this case, all coordination will be handled by MSRC and not MSVR. This is because for Microsoft as an affected vendor, the concern is affected Microsoft software and MSRC is the Microsoft program entrusted with this specific area. MSVR only becomes involved with MSRC cases if the reported vulnerability affects multiple vendors and in the event of this occurring, MSVR will coordinate as outlined in Section 2. Microsoft as a Vulnerability Coordinator.

Conclusion

While no document can envision every vulnerability scenario, these practices are intended to provide greater clarity and certainty when coordinating vulnerabilities with Microsoft. Microsoft encourages other companies and security researchers to adopt a similar approach, and work with software providers to help minimize customer risk. By working together in a coordinated manner, we are creating a safer, more trusted computing experience for our customers.