Coordinated Vulnerability Disclosure

Microsoft Policy Papers

Minimizing cybersecurity risk through coordinated vulnerability disclosure

Today's prevalence of information technology (IT) means that ensuring that products and services used are secure is a critical part of risk management for many organizations. The vast majority of that work lies in determining whether software vendors have secure development and operational measures in place, which align to established international frameworks, such as the NIST Cybersecurity Framework[1]. These practices can significantly contribute to product and service vulnerabilities being found and addressed prior to market release.

However, the complexity of modern software means that some vulnerabilities persist. It is important to note that most of these will not have any material impact on the functionality of the product. Nevertheless, they can be discovered, either through intentional investigation or accidentally and might be maliciously exploited. It is therefore important that, whenever they are found, the affected vendors are informed, enabling them to resolve the issue without exposing users to undue risk. In addition, it is important that affected vendors have a policy and process for receiving external reports about vulnerabilities. This process is commonly referred to as a *vulnerability handling policy*[2].

Coordinated vulnerability disclosure is about minimizing risk – for customers and businesses

- A *security vulnerability* is a weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product.
- An exploit is a software program or sample code that (when executed against a vulnerable system) uses one or more security vulnerabilities to cause unintended or unanticipated behavior.
- A zero-day exploit is one that takes advantage of one or more security vulnerabilities on the same day that the vulnerability or vulnerabilities become generally known.

The actors that search for and discover vulnerabilities include government agencies, software developers, IT companies, security researchers, as well as criminals. Their motivations are varied: IT companies have an interest in preserving the security and integrity of their offerings; security firms can sell the information and services that flow from it; security researchers may be pursuing academic work, aiming to improve ecosystem security, or satisfying individual curiosity; and criminals are out to exploit them.

Microsoft's approach to vulnerability disclosure and handling

Microsoft believes that coordinated disclosure most effectively minimizes risk to technology users. Under our *Coordinated Vulnerability Disclosure* policy, finders of a vulnerability report it directly to affected vendor(s) (or to coordinators that will disclose it to the vendor(s) privately), waiting to disclose it publicly until the vendor has developed, tested, and released patches or other mitigations. The vendor coordinates with the vulnerability finder throughout the investigation, remediation, and disclosure process, updating the finder as progress is made. This coordination allows the vendor to do a full investigation and offer fully tested updates or other corrective measures before vulnerability information is shared publicly, likely increasing awareness of the existence of a vulnerability and the development of a criminal exploit. If attacks using the vulnerability are detected whilst the vendor is still working on the update, though, then the finder and vendor should coordinate closely in providing early public disclosure and a comprehensive set of existing risk mitigations. The aim should be to provide timely and consistent guidance to technology users to help them protect themselves.

[1] NIST Cybersecurity Framework: https://www.freepdfconvert.com/pdf-image

[2] Two international standards reflect best practices for vulnerability disclosure and handling: ISO/IEC 29147 and ISO/IEC 30111

Microsoft

Some companies and individuals believe that, even if there is no evidence of an attack using a found vulnerability, earlier public disclosure is preferred because it forces vendors to develop mitigations more quickly. However, given the facts that vendors are in the best position to assess the risk priority of different vulnerabilities and that most users are reliant on a software provider to release a path, Microsoft believes that those who disclose a vulnerability before a fix is broadly available are doing a disservice to millions of people and the systems they depend upon. Furthermore, even for those who take action, risk is significantly increased when information that a criminal can use to orchestrate an attack is publicly released. Our research shows that of the vulnerabilities privately disclosed and fixed through coordinated disclosure practices each year by all software vendors, almost none are exploited before a "fix" has been provided to customers, and even after a "fix" is made publicly available, only a small number are ever exploited. Conversely, the track record is far worse for vulnerabilities publicly disclosed before fixes, with criminals more frequently orchestrating attacks against those who struggle to protect themselves.

Government role in security vulnerability handling

Government role in vulnerability handling is multifaceted. First and foremost, governments are central to initiating and encouraging voluntary cybersecurity *information sharing* activities by ensuring they are not subject to any legal or policy barriers. Similarly, they can advance the work of security researchers by creating *cybercrime frameworks* that address intent or clarify acceptable research behavior.

Finally, certain governments *exploit* security vulnerabilities rather than working with the vendors to fix them. The fact that governments are active participants in the security vulnerability market has been well-documented[3] and remains a concern for global security vendors and ICT companies. A decision to retain a vulnerability reduces ecosystem security, while disclosing it so it can be patched could undercut the ability of intelligence agencies to gather intelligence or the military to carry out offensive cyber operations. This situation frequently puts two different parts of the government at loggerheads: those charged with protecting the nation in cyberspace versus those focused on intelligence, law enforcement, and military missions that may require the use of such vulnerabilities.

US government vulnerabilities equities process

- The extent of the vulnerable system's use.
- The risks posed and the possible harm if the vulnerability is left unpatched.
- Whether the Administration would know if another government or organization was exploiting the vulnerability.
- Whether the vulnerability is needed to obtain intelligence.
- How likely it is that others will discover the vulnerability.
- Whether the government can use the vulnerability for a short period before disclosing it.
- Whether the vulnerability can be patched or otherwise mitigated.

In 2014, in response to specific allegations against the US government, the White House published their approach to addressing if or when the government may withhold knowledge of a vulnerability from the public.[4] Microsoft recommends that other governments similarly *develop and publish their policies on vulnerability handling*. These policies should be clear and principle-based and should reflect a strong mandate for reporting vulnerabilities to vendors rather than stockpiling, buying, selling, or exploiting them. When doing so, they should adhere to the principles of Coordinated Vulnerability Disclosure, discussed above.

[3] "The digital arms trade." The Economist. March 30, 2013. http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade

[4] White House blog: https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities