Coordinated Vulnerability Disclosure (CVD)

CEPS - Brussels, June 23, 2017

Jan Neutze
Director Cybersecurity EMEA
Microsoft

What's driving the debate about Vulnerability Disclosure?

Increasing concerns about cybersecurity

- Increasing dependence and understanding of potential risk.
- Vulnerabilities are a key attack vector.
- Not all vendors have robust patch management processes in place.
- Use of legacy systems in critical infrastructures.

Internet of Things (IoT) broadens attack surface

- 20-30 billion connected devices by 2020
- Major IT vendors have been working on CVD for more than a decade and have robust patch management processes in place.
- Many "new entrants," however, including many IoT vendors are new "technology providers" and have not started putting CVD processes in place.

What is vulnerability disclosure?

A weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product.

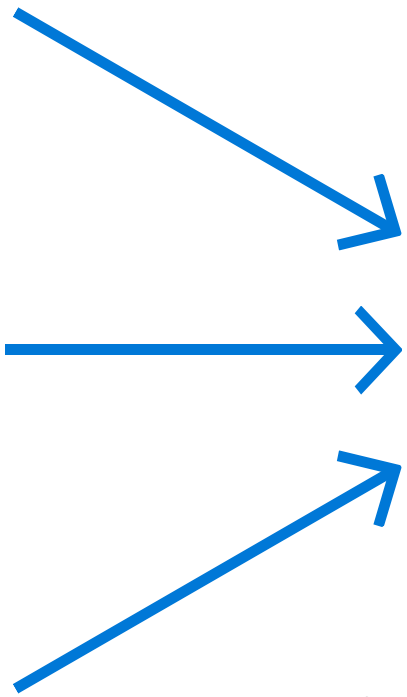
SECURITY VULNERABILITY

A software program or sample code that, when executed against a vulnerable system, uses a security vulnerability to cause unintended and/or unanticipated behavior.

EXPLOIT

An exploit that takes advantage of a security vulnerability that is not known to the vendor. There are zero days between the time the vulnerability is discovered and the first attack.

ZERO DAY EXPLOIT



VULNERABILITY DISCLOSURE…

…is the process by which someone shares information about a security vulnerability so that it can be mitigated or fixed, ideally before being exploited

Types of Vulnerability Disclosure

Type	Full Disclosure	Responsible Disclosure	Coordinated Vulnerability Disclosure	No Disclosure
Description	Public release of all the details of the vulnerability (often without mitigation information necessary to protect users)	Finders share vulnerability information with vendors, but what's "responsible" distracts from focus on the user	Finders share vulnerability information with vendors, and stakeholder focus is on coordination to protect users	Governments or vendors acquire vulnerabilities for exploit or advantage; researchers fear reprisal for sharing information
Impact	Exploitable immediately, increasing user risk; response required	Vulnerability may be released before patch/mitigation, increasing user risk	Vulnerability information released with patch/mitigation	Use in targeted attacks; can leak; incorporated into tools/platforms for sale/pen testing

Coordinated vulnerability disclosure (CVD): stakeholders and roles

Microsoft

Finders

Someone, often a security researcher, who finds and discloses newly discovered vulnerabilities directly to:

- **the vendor of the affected product or service; or,**
- **a coordinator.**

Coordinators

An organization, often a CERT/CSIRT or a bug bounty provider, that cooperatively works as an intermediary with finders and vendors to privately disclose newly discovered vulnerabilities directly to the vendor of the affected product or service.

Vendors

An organization that has a way to receive vulnerability report, coordinate with finders throughout the vulnerability investigation, provide the finder with updates on case progress, and diagnose and offer fully tested patches or other corrective measures.

CVD is about minimizing risk – for customers, businesses, and critical infrastructures.

Coordinated vulnerability disclosure (CVD): policy principles and standards

Microsoft

1) Vulnerability research is a valuable part of securing the ecosystem.
2) Vulnerability research should not cause harm.
3) Vulnerabilities are best fixed before users are impacted by them.
4) All stakeholders have responsibilities to keep users safe, including the user.

ISO 29147 – for external process of finder/vendor coordination

ISO 30111 – for vendor's internal process of investigating, diagnosing, patching

Incentivizing behavior: bug bounties

Microsoft

Other organizations are also using bug bounties, i.e.

AT&T
U.S. Dept. of Defense
Facebook
Google
Mozilla
Samsung
Tesla
Twitter
Uber
United Airlines

Online Services

- The Online Services Bug Bounty program gives individuals across the globe the opportunity to submit vulnerability reports on eligible Online Services (O365 and Microsoft Azure) provided by Microsoft.
- Being ahead of the game by identifying the exploit techniques in our widely used services helps make our customer's environment more secure.
- Qualified submissions are eligible for payment from a minimum of $500 USD up to $15,000 USD.

Mitigation Bypass Bounty

- Microsoft will pay up to $100,000 USD for truly novel exploitation techniques against protections built into the latest version of our operating system. Learning about new exploitation techniques earlier helps Microsoft improve security by leaps, instead of capturing one vulnerability at a time as a traditional bug bounty alone would.

Bounty for Defense

- Additionally, Microsoft will pay up to $100,000 USD for defensive ideas that accompany a qualifying Mitigation Bypass submission. Doing so highlights our continued support of defensive technologies and provides a way for the research community to help protect more than a billion computer systems worldwide (in conjunction with the Mitigation Bypass Bounty).

What governments are doing about it

Bringing together governments and vendors to raise awareness and share best practices around:
- The value of security research
- The importance of coordination
- Issues of legal uncertainty

Example:

-Dutch government-sponsored Global Forum on Cyber Expertise

Bringing together vendors (especially IoT) to raise awareness and share best practices around:
- The value of security research
- The importance of coordination
- The issue of legal uncertainty

Example:

-U.S. Dept. of Commerce: National Telecommunications and Information Administration (NTIA)

Increasing legal certainty for security researchers through:
- Legal exemptions
- Legal analyses

Examples:

-U.S. copyright exemptions for car, medical device research

-Dutch government interpretation of "unlawful" access

Developing government policies:
- To promote CVD
- To act as a coordinator
- To clarify vuln equities process
- To create bug bounty program

Examples:

-EU Cybersecurity Strategy 2.0?

-Japanese Basic Cyber Law update

-U.S. PATCH Act on VEP policy

-U.S. DoD CVD policy

Governments' role in disclosing vulnerabilities – an opportunity for EU leadership

Microsoft

"States should have a clear, principle-based policy for handling product and service vulnerabilities. The policy should reflect a strong mandate to report vulnerabilities to vendors rather than to stockpile, buy, sell, or exploit them."

Microsoft Cybersecurity Norms Whitepaper, December 2015

The EU – in its **revised Cybersecurity Strategy** – should outline principles for Member States to develop a European Vulnerability Equities Process with a clear partiality for reporting vulnerabilities to vendors. When doing so, they should adhere to the principles of Coordinated Vulnerability Disclosure (CVD).

Example: US Government policy

The interagency decision process considers the following points when deciding on sharing the vulnerability:

- 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.


Microsoft