Coordinated Vulnerability Disclosure

Laurie Tyzenhaus
June 2018
Coordination Communication Topologies

Common network topologies

- Full mesh
- Point-to-point
- Hub-and-spoke
- Shared bus
Single Vendor Vulnerability Report

Reporter Identifies a Vulnerability

Reporter contacts Vendor

Vendor responds (or ignores) Reporter

Reporter requests assistance:
• Reporter contacts CERT/CC
• CERT/CC confirms VUL
• CERT/CC communicates with Reporter
• CERT/CC contacts Vendor
Multiple Vendor Vulnerability Report

Hub & Spoke

C

R

V

V

V
Coordinated Vulnerability Disclosure

Problems with Multi-Vendor Coordination:

   Hub & Spoke does not scale
   Who do we notify?
   Who did we miss?
   More effort happens after Disclosure
   Vendors must contact us for updating the vul note.

Balancing conflicting vendor disclosure policies.

Examples:

   VU#484891 (the vul that enabled SQL Slammer)
   VU#228519 (KRACK)
Is there a better solution?

Improving Coordination
Collaborative Vulnerability Disclosure
A Better Solution?

Shared Bus

C

V

V

V

V

R
Microsoft’s response to Congressional Letter

In less complicated scenarios, the CVD protocol calls for a hub-and-spoke model of communication through which a vulnerability owner communicates individually with each affected vendor.

In more complicated scenarios—like the one presented by Meltdown and Spectre—a “shared-bus” model can be required, to ensure affected companies can coordinate directly “through the use of conference calls, group meetings, and private mailing lists.”

Communications

- Private shared venue
- Vendors are invited in.
- Shared file space
- Track threaded discussions
- Vendors can be added, immediate access to history
Coordinator/Coordination

- Sets target dates and milestones
- Identifies and invites affected vendors
- Invites additional vendors as identified
Reporter

- Identifies the vulnerability
- May/may not contact vendor(s)
- Contacts Coordinator
Vendors

- Vendors post statements, links to patches, etc.
- Possible Multiple vulnerability reports (separate venues)
## Challenges

<table>
<thead>
<tr>
<th>Coordination</th>
<th>Collaboration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking threaded communications</td>
<td></td>
</tr>
<tr>
<td>Secure Communications</td>
<td></td>
</tr>
<tr>
<td>Contact Management</td>
<td>Account Management?</td>
</tr>
<tr>
<td>Disclosure Timing</td>
<td>Disclosure Timing – Everyone agrees?</td>
</tr>
<tr>
<td>Publishing</td>
<td>Publishing</td>
</tr>
<tr>
<td>Updating Reports</td>
<td>Updating Reports</td>
</tr>
</tbody>
</table>
## Alternate Disclosure

<table>
<thead>
<tr>
<th>Pre-Disclosure:</th>
<th>Disclosure:</th>
<th>Post – Disclosure:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group effort</td>
<td>Artifacts (publishable docs)</td>
<td>Find new vendors</td>
</tr>
<tr>
<td>Open comms within the group</td>
<td></td>
<td>Update references</td>
</tr>
<tr>
<td>Add new vendors</td>
<td></td>
<td>Refine Content</td>
</tr>
<tr>
<td>Discussion threads/ scheduling disclosure</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Who does Multi-Vendor Coordination?

More organizations than expected...
Who does Multi-Vendor Coordination?

Microsoft
Intel
Google
CERT/CC
Other CERTs
PSIRTs
Microsoft

Coordinated Vulnerability Disclosure


Minimizing cybersecurity risk through coordinated vulnerability disclosure


A Call for Better Coordinated Vulnerability Disclosure

https://blogs.technet.microsoft.com/msrc/2015/01/11/a-call-for-better-coordinated-vulnerability-disclosure/
Product Security at Intel


Bug Bounty Program


Vulnerability handling Guidelines

Google

Google Vulnerability Reward Program (VRP) Rules
https://www.google.com/about/appsecurity/reward-program/

HackerOne – bug bounty program
https://hackerone.com/google
https://www.google.com/about/appsecurity/reward-program/

How Google handles security vulnerabilities
https://www.google.com/about/appsecurity/
Dell

Report a Potential Vulnerability in Dell Products or Software


HackOne

https://hackerone.com/dellsecureworks
HP

Report a potential security vulnerability to HP (reporting form)

HackerOne
https://hackerone.com/hp

HP Enterprise Product Security Vulnerability Alerts
The CERT® Guide to Coordinated Vulnerability Disclosure

https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf


Guidelines for Requesting Coordination Assistance

https://vuls.cert.org/confluence/display/Wiki/Guidelines+for+Requesting+Coordination+Assistance

Vulnerability Notes Database

https://www.kb.cert.org/vuls/

CERT Vulnerability Data Archive & Tools

https://vuls.cert.org/confluence/display/tools/CERT+Vulnerability+Data+Archive+and+Tools
Cybersecurity Tech Accord
Cybersecurity Tech Accord

34 companies committed to:
1. Stronger Defense
2. No offense
3. Capacity building
4. Collective action

Background
https://cybertechaccord.org/

Agreement
https://cybertechaccord.org/accord/
Collective Action

“The companies will build on existing relationships and together establish new formal and informal partnerships with industry, civil society and security researchers to improve technical collaboration, coordinate vulnerability disclosures, share threats and minimize the potential for malicious code to be introduced into cyberspace.”
# SIGNATORIES

<table>
<thead>
<tr>
<th>ABB</th>
<th>FACEBOOK</th>
<th>NIELSEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARM</td>
<td>FASTLY</td>
<td>NOKIA</td>
</tr>
<tr>
<td>AVAST</td>
<td>FIREEYE</td>
<td>ORACLE</td>
</tr>
<tr>
<td>BITDEFENDER</td>
<td>F-SECURE</td>
<td>RSA</td>
</tr>
<tr>
<td>BT</td>
<td>GITHUB</td>
<td>SAP</td>
</tr>
<tr>
<td>CA TECHNOLOGIES</td>
<td>GUARDTIME</td>
<td>STRIPE</td>
</tr>
<tr>
<td>CARBON BLACK</td>
<td>HP INC</td>
<td>SYMANTEC</td>
</tr>
<tr>
<td>CISCO</td>
<td>HPE</td>
<td>TEELFONICA</td>
</tr>
<tr>
<td>CLOUDFLARE</td>
<td>INTUIT</td>
<td>TENABLE</td>
</tr>
<tr>
<td>DATASTAX</td>
<td>JUNIPER NETWORKS</td>
<td>TRENDMICRO</td>
</tr>
<tr>
<td>DELL</td>
<td>LINKEDIN</td>
<td>VMWARE</td>
</tr>
<tr>
<td>DOCUSIGN</td>
<td>MICROSOFT</td>
<td></td>
</tr>
</tbody>
</table>
What can you do today?

1. Provide current contact information for vulnerability reports.
   - generic email address
   - group that monitors incoming messages
2. Maintain PGP key(s).
3. Share this information with CERT organizations.
What are your thoughts?

Laurie Tyzenhaus
latyzenhaus@cert.org

Coordinated Vulnerability Disclosure
Team Lead