Coordinated Vulnerability Disclosure

Laurie Tyzenhaus
February 2018
Copyright 2018 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon®, CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM18-0315
Reminder – RSA Attendees

VENDOR Meeting: Monday April 16, 2018, Westin St. Francis in San Francisco, CA, US.

FREE

https://www.eventbrite.com/e/2018-cert-vendor-meeting-registration-39956032569

Morning Sessions:

1. Training: Vul Coordination 101
2. Supply chain transparency & component relationships

Afternoon Session:

Radically new ways multi-party coordinated vulnerability disclosure
Coordination Communication Topologies

Common network topologies
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

Diagram:

- C (CERT/CC)
- V (Vendor)
- R (Reporter)

Point to Point
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: Artifacts (publishable docs)</th>
<th>Post – Disclosure:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group effort</td>
<td></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/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>scheduling disclosure</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What are your thoughts?

Laurie Tyzenhaus
latyzenhaus@cert.org

Coordinated Vulnerability Disclosure
Team Lead