# Coordinated Vulnerability Disclosure

Laurie Tyzenhaus

June 2018

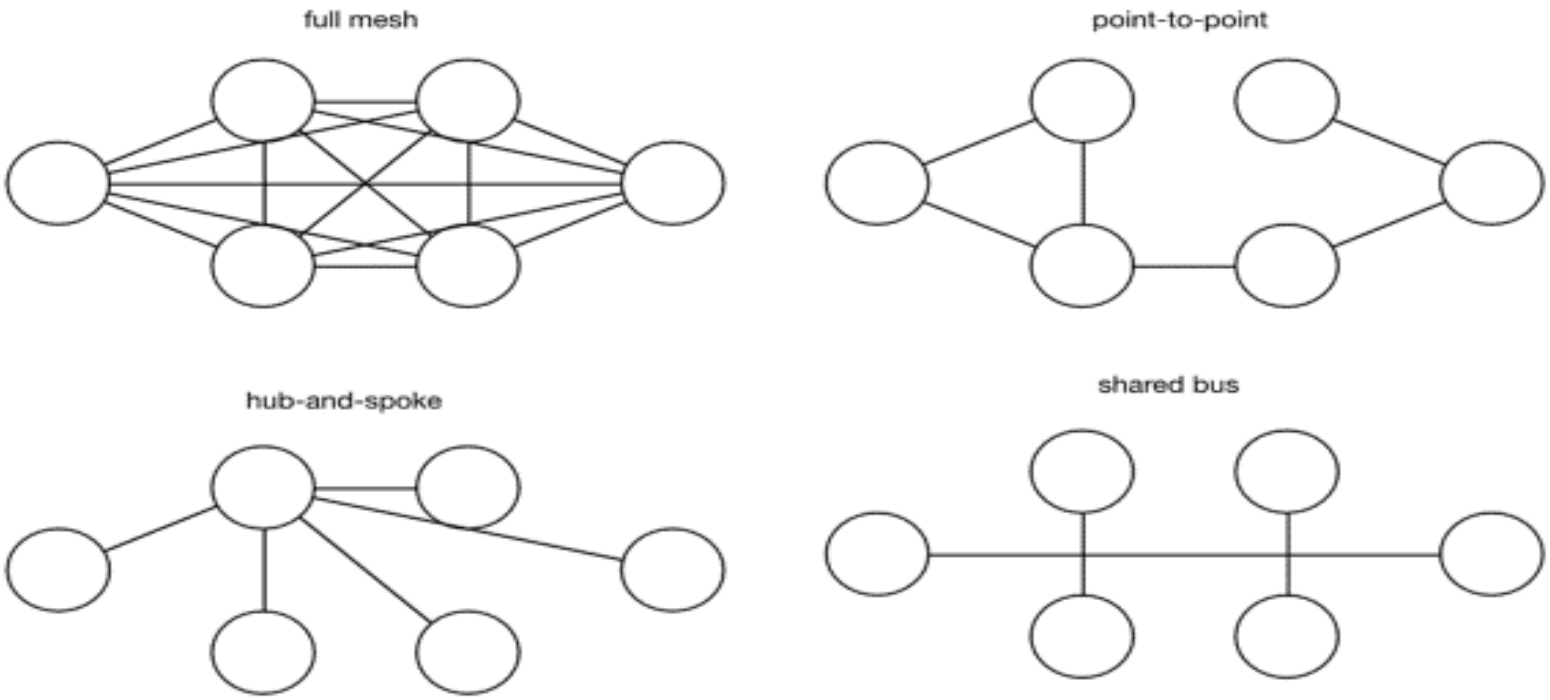
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Homeland Security 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 sponsored by the United States Department of Defense.



DM18-0777

# Coordination Communication Topologies




**Common network topologies**

# Single Vendor Vulnerability Report

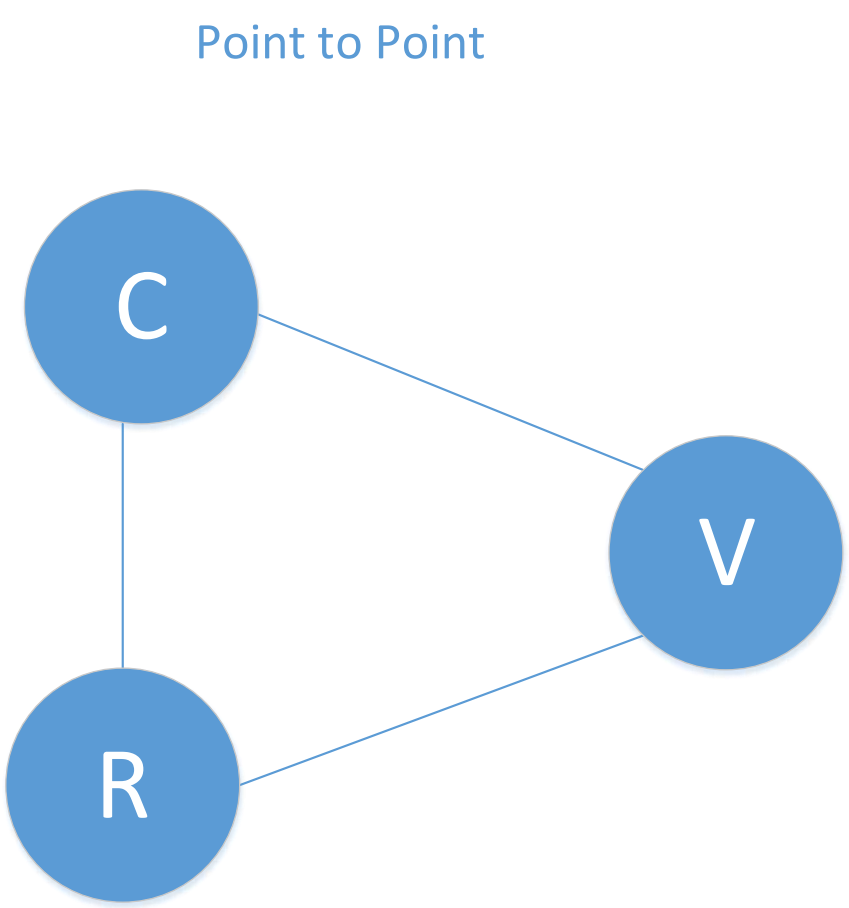
Reporter Identifies a Vulnerability

Reporter contacts Vendor

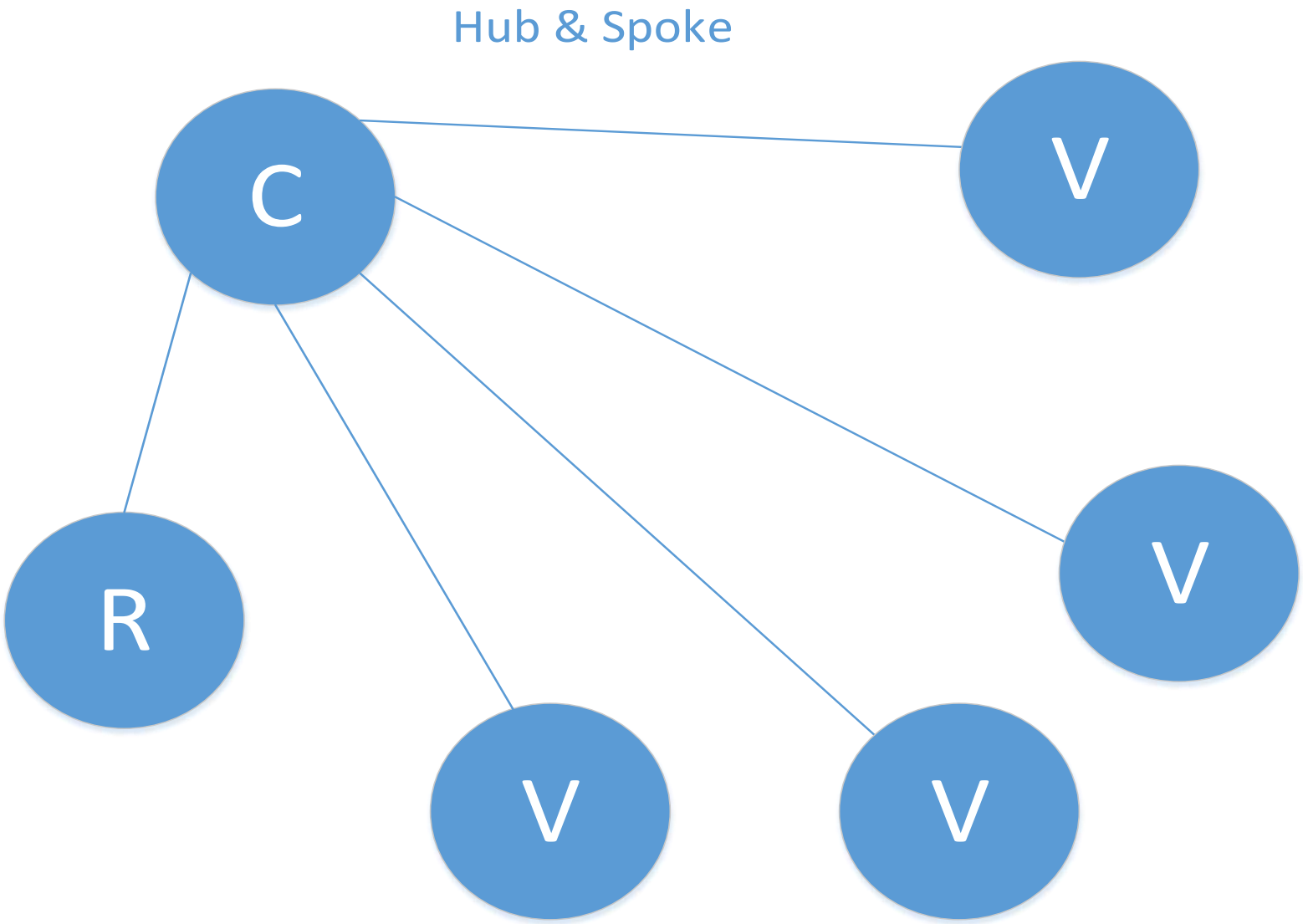
Vendor responds (or ignores) Reporter

Reporter requests assistance:

- Reporter contacts CERT/CC
- CERT/CC confirms VUL
- CERT/CC communicates with Reporter
- CERT/CC contacts Vendor



# Multiple Vendor Vulnerability Report



# 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:

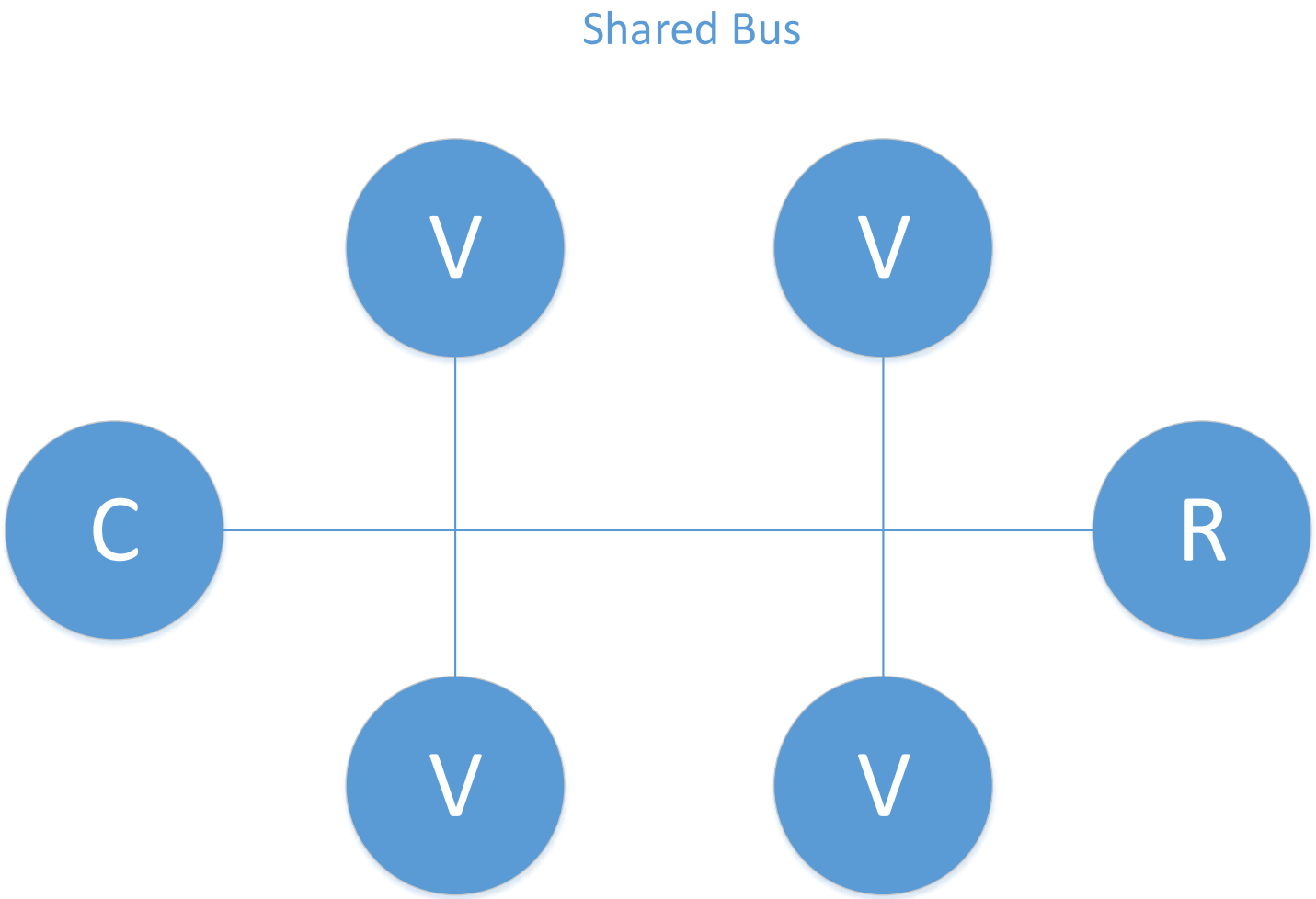
- VU#484891 (the vul that enabled SQL Slammer)
- VU#228519 (KRACK)

Is there a better solution?

# Improving Coordination

# Collaborative Vulnerability Disclosure

# A Better Solution?



# Microsoft's response to Congressional Letter

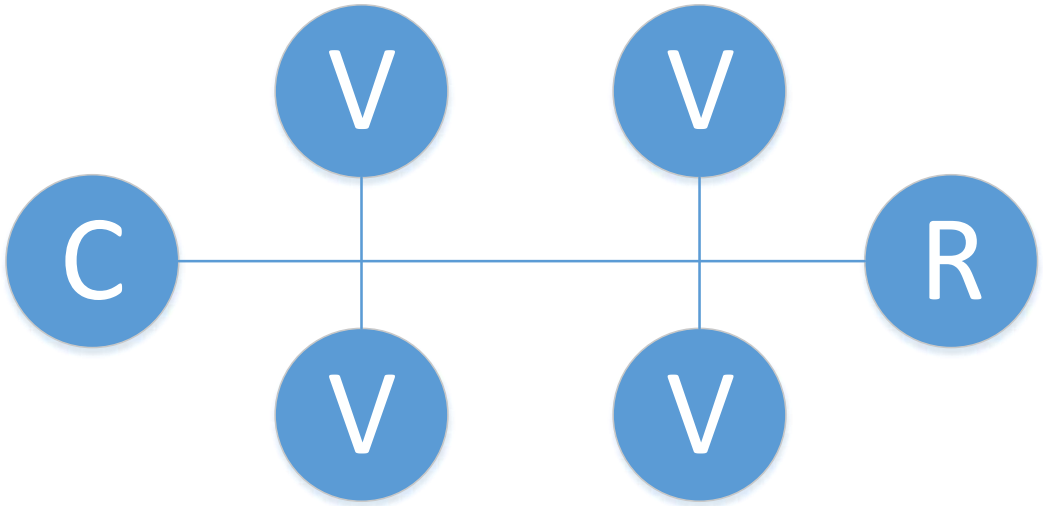
In less complicated scenarios, the CVD protocol calls for a **hub-and-spoke** model of communication through which a vulnerability owner communicates individually with each affected vendor.

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."

https://energycommerce.house.gov/wp-content/uploads/2018/02/MSFT-Spectre-Response-to-EC-Committee-.pdf

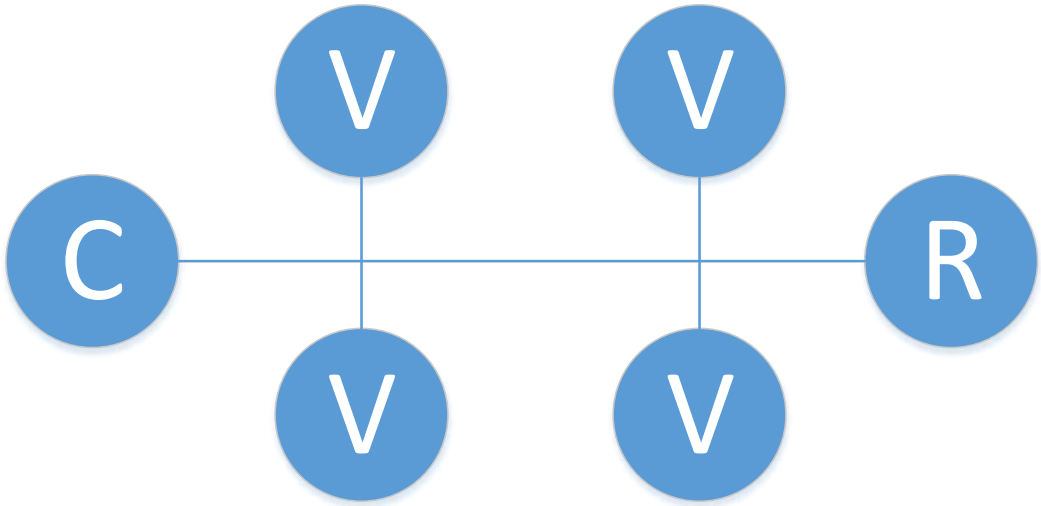
# Communications

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



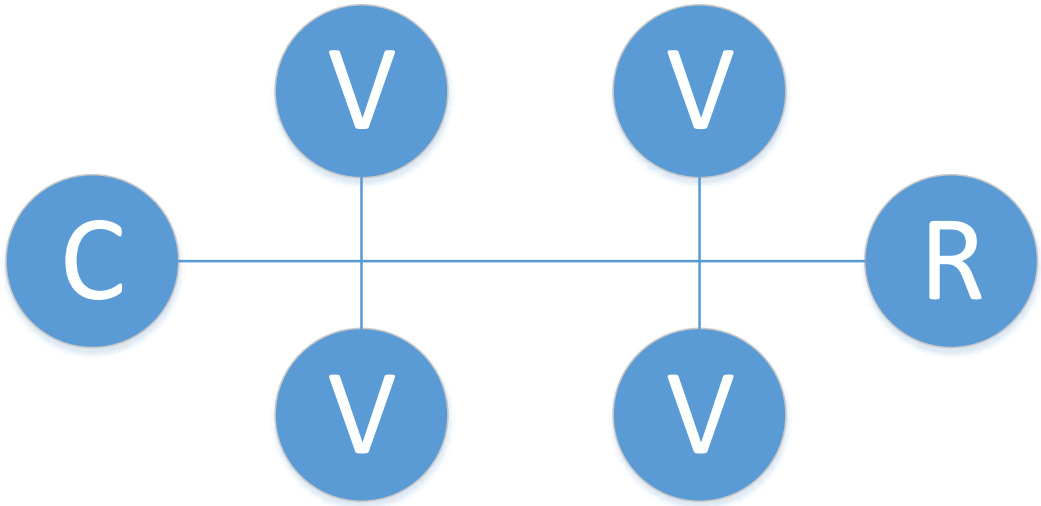
# Coordinator/Coordination

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



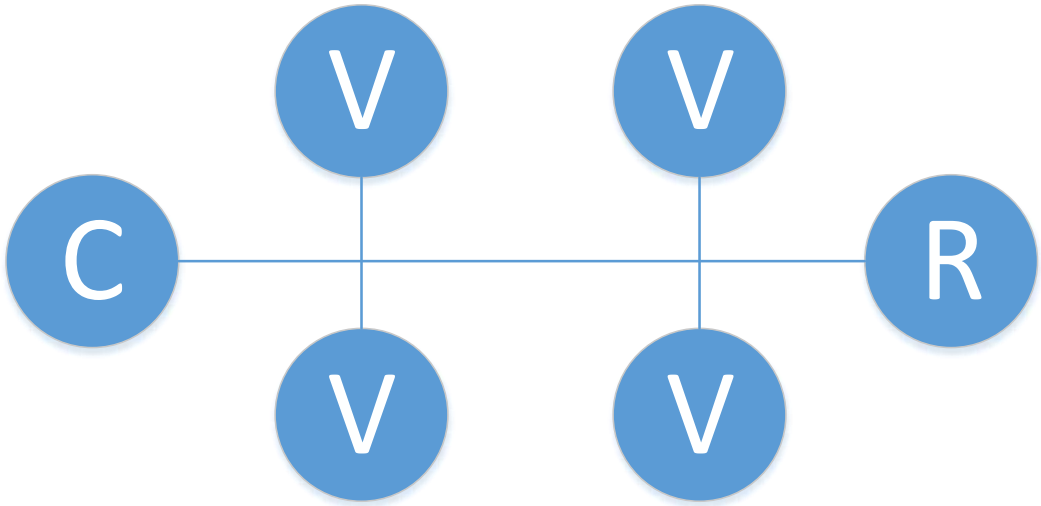
# Reporter

- 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

| Coordination | Collaboration |
| --- | --- |
| Tracking threaded communications | |
| Secure Communications | |
| Contact Management | Account Management? |
| Disclosure Timing | Disclosure Timing – Everyone agrees? |
| Publishing | Publishing |
| Updating Reports | Updating Reports |
| | |

# Alternate Disclosure

| Pre-Disclosure : | Disclosure: | Post – Disclosure: |
| --- | --- | --- |
| Group effort<br>Open comms within the group<br>Add new vendors<br>Discussion threads/ scheduling disclosure | Artifacts<br>(publishable docs) | Find new vendors<br>Update references<br>Refine Content |

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**

https://technet.microsoft.com/en-us/security/dn467923.aspx

**Minimizing cybersecurity risk through coordinated vulnerability disclosure**

https://www.microsoft.com/en-us/cybersecurity/content-hub/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/

# Intel

Product Security at Intel

https://www.intel.com/content/www/us/en/corporate-responsibility/product-security.html

Bug Bounty Program

https://www.intel.com/content/www/us/en/security-center/bug-bounty-program.html

Vulnerability handling Guidelines

https://www.intel.com/content/www/us/en/security-center/vulnerability-handling-guidelines.html

# 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

https://www.dell.com/learn/us/en/04/campaigns/report-vulnerability

HackOne

https://hackerone.com/dellsecureworks

# HP

**Report a potential security vulnerability to HP (reporting form)**

https://ssl.www8.hp.com/h41268/live/index.aspx?qid=25434

HackerOne

https://hackerone.com/hp

HP Enterprise Product Security Vulnerability Alerts

https://www.hpe.com/us/en/services/security-vulnerability.html

The CERT® Guide to Coordinated Vulnerability Disclosure

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

Report a vulnerability (form) https://vulcoord.cert.org/VulReport/

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

ABB
ARM
AVAST
BITDEFENDER
BT
CA TECHNOLOGIES
CARBON BLACK
CISCO
CLOUDFLARE
DATASTAX
DELL
DOCUSIGN
FACEBOOK
FASTLY
FIREEYE
F-SECURE
GITHUB
GUARDTIME
HP INC
HPE
INTUIT
JUNIPER NETWORKS
LINKEDIN
MICROSOFT
NIELSEN
NOKIA
ORACLE
RSA
SAP
STRIPE
SYMANTEC
TEELFONICA
TENABLE
TRENDMICRO
VMWARE

# 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