

# ESTABLISHING A GLOBAL COMMUNITY OF PRACTICE ON COORDINATED VULNERABILITY DISCLOSURE

June 27<sup>TH</sup>, 2025

Justin Murphy  
CISA

Tomo Ito  
JPCERT/CC



TLP:CLEAR



# Who are we?



Tomo Ito

- Global CVD Project Lead @ JPCERT/CC
- Passion for:
  - CVD
  - SBOM/VEX
  - CVE
  - International Cooperation



Justin Murphy

- Vulnerability Analyst @ CISA
- Passion for:
  - CVD
  - SBOM/VEX
  - CSAF/OpenEoX
  - International Cooperation

# Today's Presentation

- Global Community of Practice on Coordinated Vulnerability Disclosure (CVD-COP)
  - CVD Overview
  - Global CVD-COP
    - Objectives
    - Why?
    - Membership
    - Opportunities & Challenges
    - Vision & Future Work
  - Discussion



TLP:CLEAR

JPCERT/CC<sup>®</sup>

# CVD

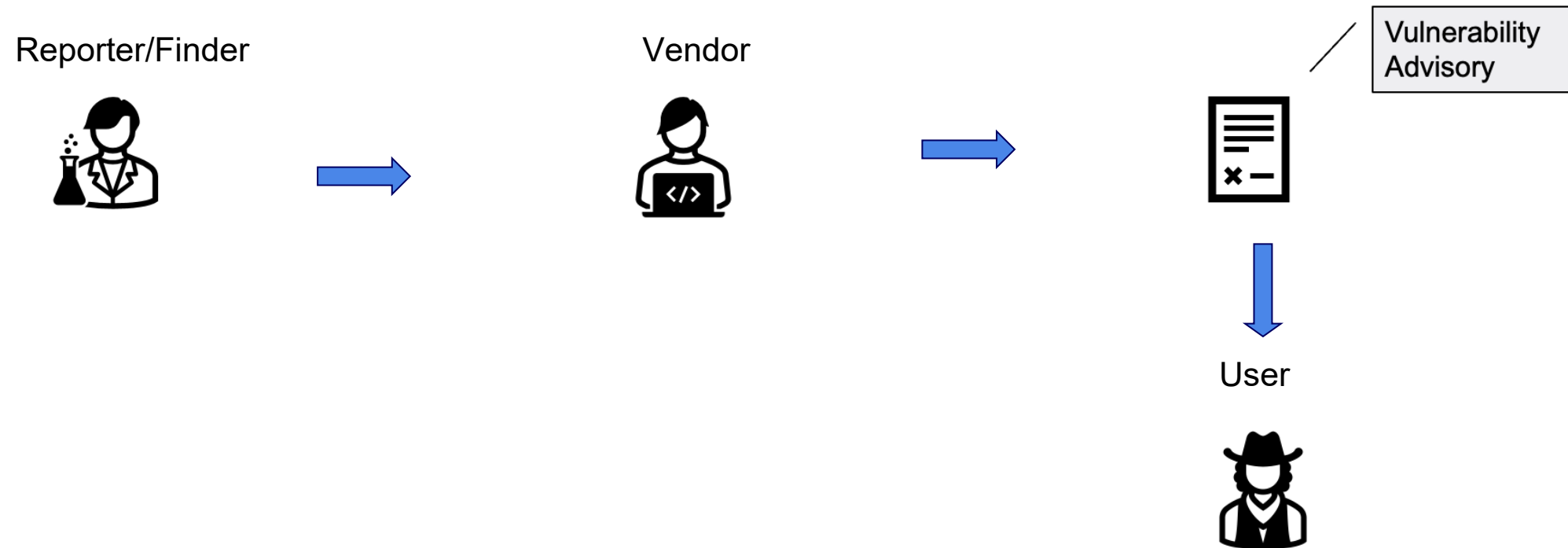
- Coordinated Vulnerability Disclosure (CVD)
  - Gathering, coordinating, and disclosing of vulnerability information
  - It is a global good practice
  - Often many different stakeholders are involved in CVD cases
  - Vulnerability information flows through global product supply chain
  - Multi-Party CVD (MPCVD) complexity = Supply chain complexity
- The importance of CVD increasing



TLP:CLEAR

JPCERT/CC<sup>®</sup>

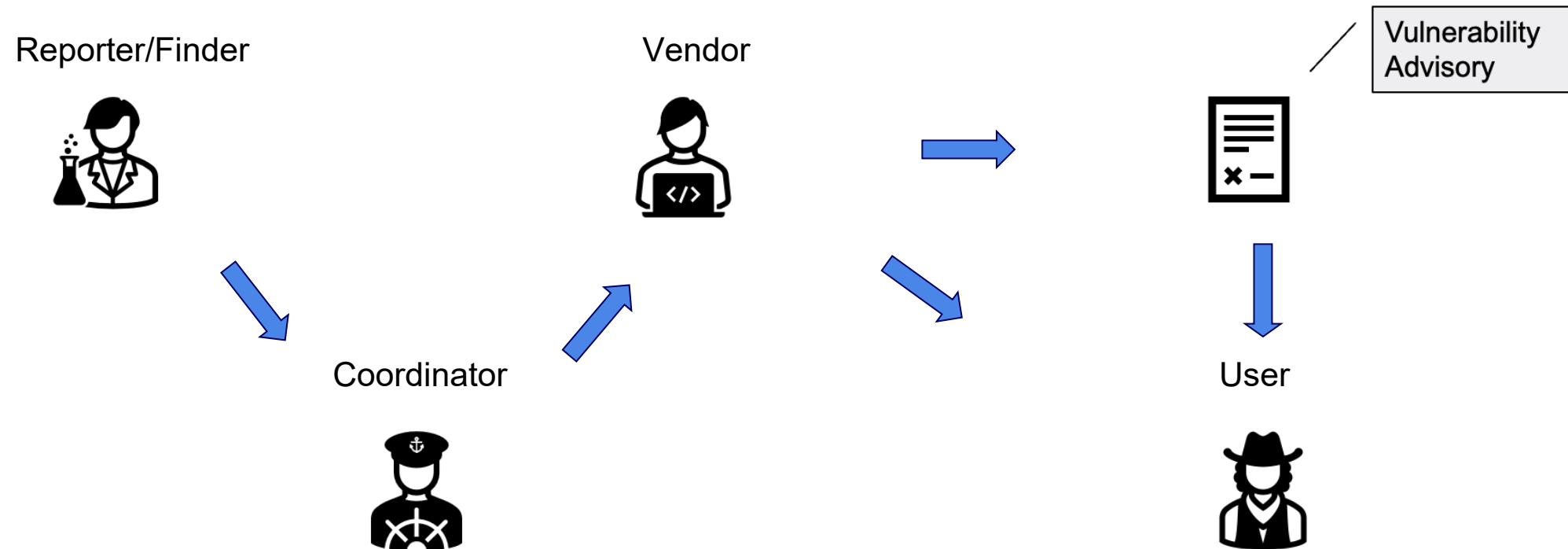
# Basic stakeholders and information flow



TLP:CLEAR

JPCERT/CC

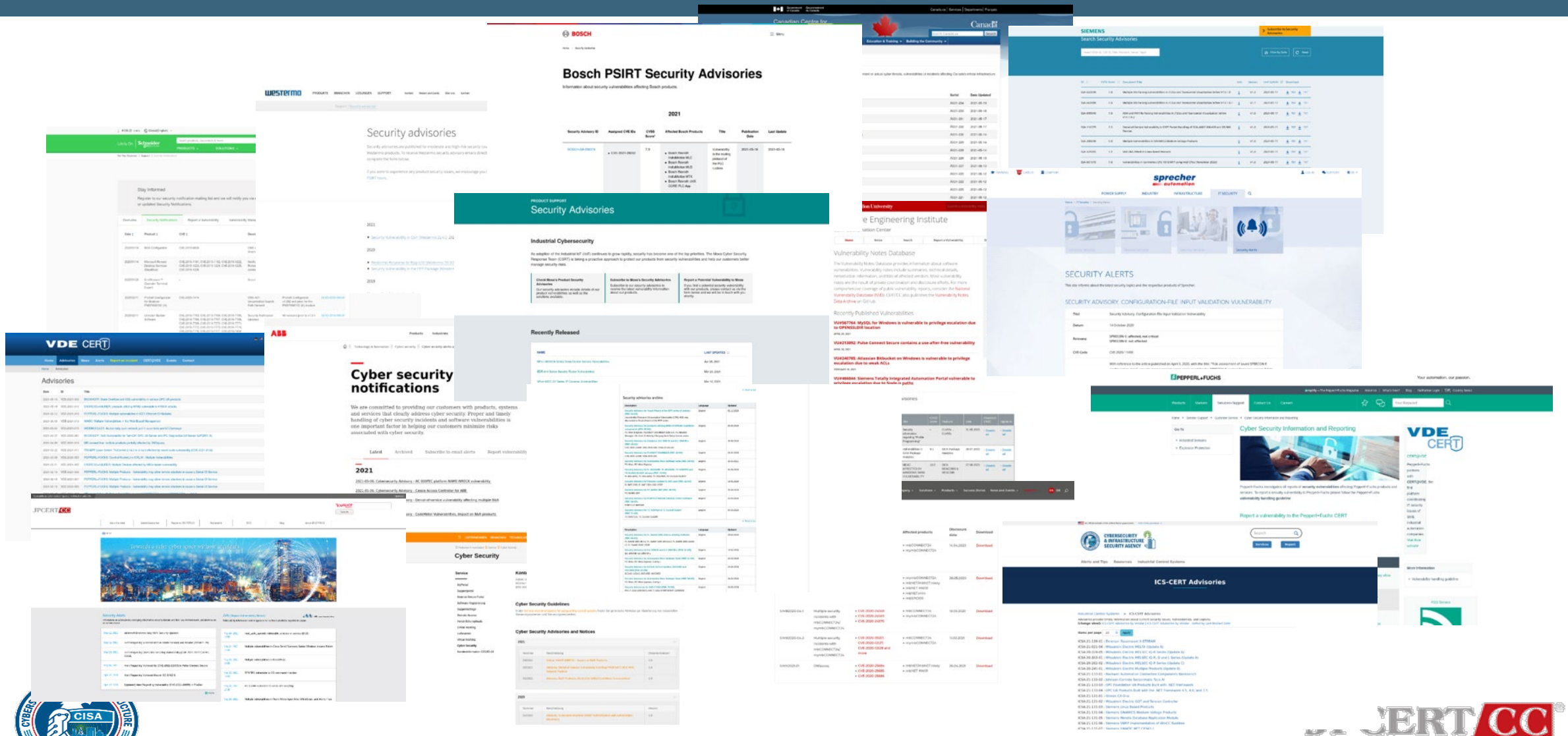
# Basic stakeholders and information flow



TLP:CLEAR

JPCERT/CC

# Advisory Examples



TLP:CLEAR

# Advisory Example

## Products Affected

- Special Interest Group Network for Analysis and Liaison versions 4.4.0 to 4.7.7



TLP:CLEAR

JPCERT/CC<sup>®</sup>



# Advisory Example

## Products Affected

### Description

Special Interest Group Network for Analysis and Liaison's "Inter-SOC Cooperation API" provided by Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) contains multiple vulnerabilities listed below.



TLP:CLEAR

JPCERT/CC®

# Advisory Example

- **Improper Authorization in Information Provision function (CWE-285) - CVE-2023-38751**

CVSS v3 CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N Base Score: 3.5

CVSS v2 AV:N/AC:L/Au:S/C:P/I:N/A:N Base Score: 4.0

- **Improper Authorization in Information Provision and Group Message functions (CWE-285) - CVE-2023-38752**

CVSS v3 CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N Base Score: 3.5

CVSS v2 AV:N/AC:L/Au:S/C:P/I:N/A:N Base Score: 4.0

/CC) contains



TLP:CLEAR



# Advisory Example

Products Affected		• Improper Authorization in Information Provision function (CWE-285) - CVE-2023-38751	
Impact			
<ul style="list-style-type: none"><li>Organization information of the information receiver that is set as "non-disclosure" in the information provision operation may be viewed by an authorized API user - CVE-2023-38751</li><li>Attribute information of the poster that is set as "non-disclosure" in the system settings may be viewed by an authorized API user - CVE-2023-38752</li></ul>			
Description Special Interest Group N multiple vulnerabilities listed	CVSS v3	CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N	/CC) contains
	CVSS v2	AV:N/AC:L/Au:S/C:P/I:N/A:N	
	Base Score: 3.5		
	Base Score: 4.0		



# Advisory Example

Impact

## Solution

### Apply the Patch

Apply the patch according to the information provided by the developer.  
For more information, contact the developer.

### Apply the workaround

If the patch cannot be applied, applying the following workaround may mitigate the impacts of these vulnerabilities.

- Configure to stop using the API

8751

De

Sp

mu



TLP:CLEAR

JPCERT 

# Advisory Example

Impact

Solution

Apply the Patch

er - CVE-2023-38751

## Credit

yusuke negishi of JPCERT/CC Platform Service Group reported these vulnerabilities to JPCERT/CC. JPCERT/CC coordinated with the developer under Information Security Early Warning Partnership.

De

- Configure to stop using the API

Sp

multiple vulnerabilities li

CVSS V2: AV:N/AC:L/Au:S/C:T/I:N/X:N

Base Score: 4.0

ains



JPCERT/CC®

TLP:CLEAR

# Advisory Example

**Impact**

**Solution**

**Apply the Patch**

Apply the patch to the affected systems.

For more information, see the following link:

**Apply the workaround**

If the patch cannot be applied, the following workarounds can be used:

- Configure the system to use the following settings:

Details: This advisory contains multiple vulnerabilities listed in the following table:

CVE ID	CVSS V2	AV:N/AC:L/Au:S/C:T/I:N/X:N	Base Score	Severity
CVE-2023-38751	4.0			Medium
CVE-2023-38752	4.0			Medium

For more information, see the following link:

For more information, see the following link:

For more information, see the following link:

For more information, see the following link:

For more information, see the following link:

For more information, see the following link:

For more information, see the following link:

For more information, see the following link:

For more information, see the following link:



TLP:CLEAR

# Advisory Example

```
1  {
2    "document": {
3      "title": "Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability",
4      "category": "Cisco Security Advisory",
5      "csaf_version": "2.0",
6      "publisher": {
7        "category": "vendor",
8        "contact_details": "Emergency Support:\n+1 877 228 7302 (toll-free within North America)\n+1 408
9        "issuing_authority": "Cisco product security incident response is the responsibility of the Cisco
10       "name": "Cisco PSIRT",
11       "namespace": "https://www.cisco.com"
12     },
13     "tracking": {
14       "id": "cisco-sa-20180328-smi2",
15       "status": "final",
16       "version": "3.0.0",
17       "revision_history": [
18         {
19           "number": "1.0.0",
20           "date": "2018-03-28T15:17:05Z",
21           "summary": "Initial public release."
```

r - CVE-2023-38751

PCERT/CC.  
Partnership.

tains



TLP:CLEAR

JPCERT/CC®

# CVD is Global

- Coordinated Vulnerability Disclosure (CVD)
  - Gathering, coordinating, and disclosing of vulnerability information
  - It is a **global** good practice
  - Often many different stakeholders are involved in CVD cases
  - Vulnerability information flows through **global** product supply chain
  - Multi-Party CVD (MPCVD) complexity = Supply chain complexity
- The importance of CVD increasing







TLP:CLEAR

JPCERT/CC<sup>®</sup>



# Current State of CVD

- CVD is global – a good thing but presents challenges
  - Similar but different
  - Cultural gaps/language barriers
  - Cooperation/collaboration/harmonization a must
- CVE and CVD
  - # of Vulnerabilities  , # of CVEs  , # of CNAs 
  - Importance of CVD 
- CVD = risk reduction activity



TLP:CLEAR

JPCERT 

# CVD Coordinator

- 3rd-party coordinator for CVD
- When problems arise, acts as a mediator
- Provides opinions when needed
- Supports and often leads CVD cases
- CERTs, Governments, Bug Bounty...



TLP:CLEAR

JPCERT/CC<sup>®</sup>

# Another working group?



TLP:CLEAR

JPCERT **CC**

# What's already out there?

Software Engineering Inst  
Carnegie Mellon University

## The CERT® Guide Coordinated Vulnerability Disclosure

Allen D. Householder  
Garret Wassermann  
Art Manion  
Chris King

August 2017

SPECIAL REPORT  
CMU/SEI-2017-SR-022

CERT Division

Distribution Statement A: Approved for Public Release

<http://www.sei.cmu.edu>

## NATIONAL INFRASTRUCTURE ADVISORY COUNCIL

### VULNERABILITY DISCLOSURE FRAMEWORK

### FINAL REPORT AND RECOMMENDATIONS BY THE COUNCIL

JANUARY 13, 2004

JOHN T. CHAMBERS  
WORKING GROUP CHAIR  
CHAIRMAN AND CHIEF EXECUTIVE OFFICER  
CISCO SYSTEMS, INCORPORATED

AND

JOHN W. THOMPSON  
WORKING GROUP CHAIR  
CHAIRMAN AND CHIEF EXECUTIVE OFFICER  
SYMANTEC CORPORATION



## Good Practice Guide on Vulnerability Disclosure From challenges to recommendations

NOVEMBER 2015

Guidelines  
and Disclosures  
<https://www.enisa.europa.eu>

[www.enisa.europa.eu](http://www.enisa.europa.eu)

European Union Agency For Network And Information Security



EUROPEAN UNION AGENCY  
FOR CYBERSECURITY



TY  
S



JPCERT/CC

TLP:CLEAR

# What's already out there?



## The CERT® Guide to Coordinated Vulnerability Disclosure

Allen D. Householder  
Garret Wassermann  
Art Manion  
Chris King

August 2017

SPECIAL REPORT  
CMU/SEI-2017-SR-022

CERT Division

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

<http://www.sei.cmu.edu>

## Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges

*Report of a CEPS Task Force*



Chair: Marietje Schaake  
Rapporteurs: Lorenzo Pupillo  
Afonso Ferreira  
Gianluca Varisco



TLP:WHITE

## Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure

Spring 2020

Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure  
<https://www.first.org>

1 of 31

TLP:WHITE



## DEVELOPING NATIONAL VULNERABILITY PROGRAMMES

Challenges and initiatives  
FEBRUARY 2023



TLP:CLEAR



# What's already out there?

Software Engineering Institute  
Carnegie Mellon University

## The CERT® Guide to Coordinated Vulnerability Disclosure

Allen D. Householder  
Garret Wassermann  
Art Manion  
Chris King

August 2017

## Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges

*Report of a CEPS Task Force*



TLP:WHITE

## Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure

Spring 2020

Guidelines and Practices for Multi-Party Vulnerability Coordination  
and Disclosure  
<https://www.first.org>

TLP:WHITE

1 of 31



EUROPEAN UNION AGENCY  
FOR CYBERSECURITY

## DEVELOPING NATIONAL VULNERABILITY PROGRAMMES

Challenges and initiatives  
FEBRUARY 2023



## ISO/IEC 29147:2018

Information technology  
— Security techniques —  
Vulnerability disclosure

**Published** (Edition 2, 2018)

This publication was last reviewed and confirmed  
in 2024. Therefore this version remains current.



TLP:CLEAR

# What's already out there?

[About FIRST](#)[Membership](#)[Initiatives](#)[Standards & Publications](#)[Events](#)[Education](#)[Blog](#)[Member Portal](#)

## Initiatives

- Special Interest Groups (SIGs)
  - SIGs Framework
  - Academic Security SIG
  - AI Security SIG
  - Automation SIG
  - Big Data SIG
  - Common Vulnerability Scoring System (CVSS-SIG)
  - CSIRT Framework Development SIG
  - Cyber Insurance SIG
  - Cyber Threat Intelligence SIG
  - Digital Safety SIG
  - DNS Abuse SIG
  - Ethics SIG

## Vulnerability Coordination SIG Mission

Historically, foundational work on best practices, policy and process for vulnerability disclosure focused on bi-lateral coordination and did not adequately address the current complexities of multi-party vulnerability coordination. Factors such as a vibrant open source development community, the proliferation of bug bounty programs, third party software, supply chain vulnerabilities, and the support challenges facing CSIRTs and PSIRTs are just a few of the complicating aspects.

The Industry Consortium for Advancement of Security on the Internet, [ICASI](#), proposed to the FIRST Board of Directors that a Special Interest Group (SIG) be considered on Vulnerability Disclosure. After holding meetings at the FIRST Conferences in Boston in June 2014, ICASI formally requested FIRST to charter a SIG to review and update vulnerability coordination guidelines.

No single entity or group of stakeholders has tried to solve this coordination challenge, as it requires a multi-faceted perspective looking at working a multi-stakeholder solution.

The Vulnerability Coordination SIG is chartered to do this.

We took the opportunity to create a community-led work group to address the challenges and opportunities related to handling these issues and develop a multi-faceted solution.

## Downloads

**Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure**

English

- [v1.1 HTML Format](#)
- [v1.1 PDF Format](#)



TLP:CLEAR

# What's already out there?



TLP:WHITE



## APCERT CVD WG Starting members

### ■ 6 Asia Pacific CSIRT/Coordinator organizations:

- CERT-In
- KrCERT/CC
- TWCERT/CC
- Cybersecurity Malaysia
- AusCERT
- JPCERT/CC

\*CVD WG currently limited to APCERT Operational Members



Rapporteurs: Lorenzo Pupillo  
Afonso Ferreira  
Gianluca Varisco

Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure  
<https://www.first.org>

TLP:WHITE

1 of 31

## PROGRAMMES

Challenges and initiatives

FEBRUARY 2023



TLP:CLEAR



# Justification

- “Due to the global nature of the internet, coordinated vulnerability disclosure needs to be adopted at an international level.”
- “...vulnerability discovery, disclosure, and remediation is important to national interests. These cybersecurity issues have been global for quite some time.
- “Harmonization of CVD practices, coordination and international cooperation among players are essential priorities.”
- “...alignment of policies with existing international standards can greatly help in promoting harmonization.”



TLP:CLEAR

JPCERT/CC<sup>®</sup>

# Purpose

- ~~NCSIP Initiative 3.3.3~~
- CVD is a global good practice
- Facilitate knowledge and experience sharing/exchange.
- Enhance global/international cooperation.
- Jointly develop capacity to deal with global CVD challenges.
  - CVD cases may fail due to cultural/social/language gaps between different regions or stakeholders.
  - CVD Readiness - “Getting together to get better”



TLP:CLEAR

JPCERT **CC**

# Vision

Our vision is a world where nations work collaboratively to advance Coordinated Vulnerability Disclosure (CVD) readiness, establishing strong relationships and communication channels, ensuring the timely mitigation of vulnerabilities and reducing societal risk.

“Getting together to get better”



TLP:CLEAR

JPCERT/CC<sup>®</sup>

# Current State

- Officially established December 5<sup>th</sup>, 2024.
- Co-chairs:
  - Justin Murphy (CISA), Tomo Ito (JPCERT/CC), and Ollie N (NCSC-UK)
- Community charter finalized.
- Membership – limited to government entities or entities who perform work for the government in an official capacity (i.e. CERTs).

**Please Note:**

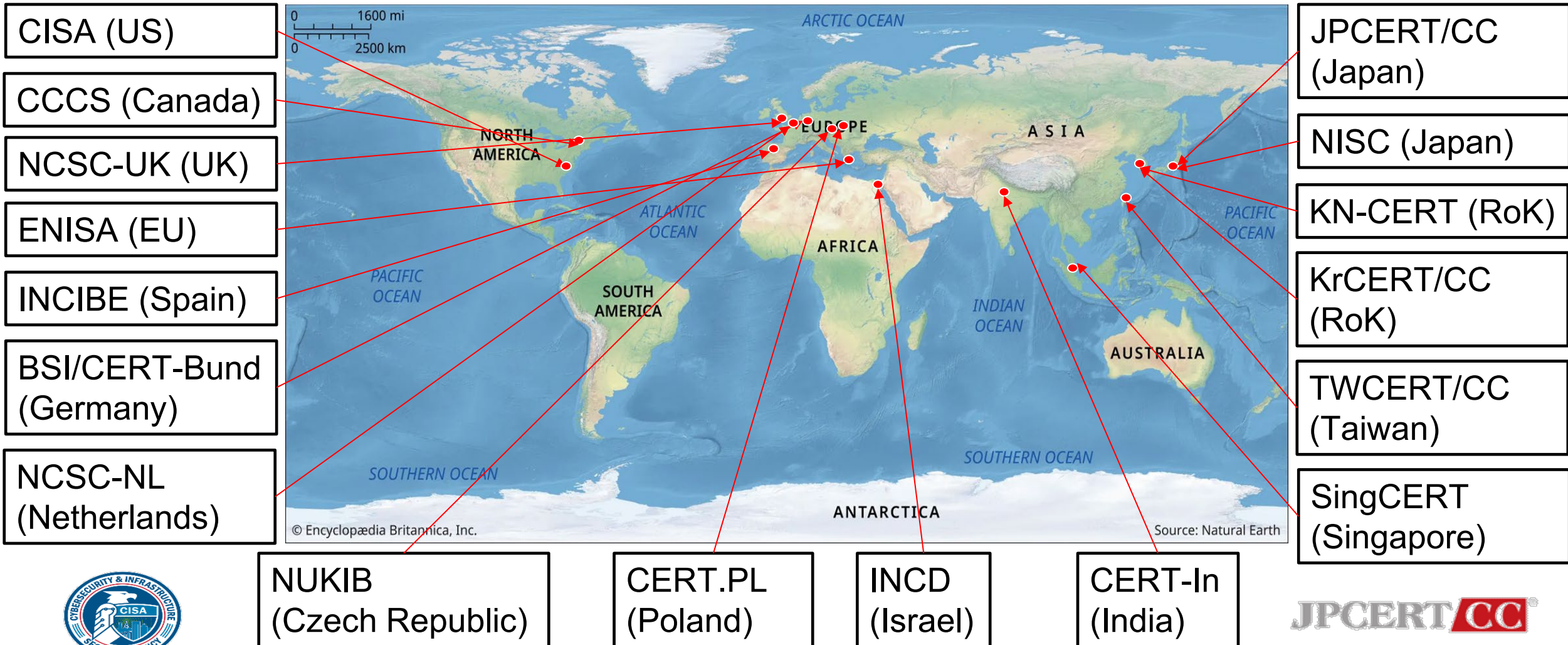
- All meeting subjects and discussion operate at **TLP:GREEN**.
- Meeting(s) are not recorded.
- Notes are taken and shared with community members.



TLP:CLEAR



# Participants



# Challenges Spotted thus Far

- Different “CVD” for different members
- Different level of understanding
- More vocal & less vocal organizations exist
- Mainly government (related) organizations – needs to be balanced with the different stakeholders in the ecosystem



TLP:CLEAR



# What We've Been Up To

- Member Presentations
- 5 potential deliverables (intended to be **TLP:CLEAR**):
  - FAQ
  - Escalation
  - Best Practices Guide
  - Lessons Learned
  - Legal Challenges



**TLP:CLEAR**

**JPCERT/CC**

# Summary

- CVD is a global good practice
- CVD is important to national interests.
- CVD Readiness
  - Global CVD-COP: CVD coordinators coming together to get better
- Aim to enhance the effectiveness of CVD globally



TLP:CLEAR

JPCERT **CC**



# Questions to the audience

- What do you see as most needed in practice?
  - What gaps exist in CVD?
  - What challenges need to be addressed in CVD?
- How might you envision our global CVD-COP supporting the CVD community?
- How can we involve different parts of the community?
- How can the community benefit from our group?

Even though it is Friday, please come and find us, we'd love to chat more about CVD!



TLP:CLEAR



**Questions?**

**Contacts:**

**Tomo Ito**

**[tomotaka.itou@jpcert.or.jp](mailto:tomotaka.itou@jpcert.or.jp)**

**Justin Murphy**

**[justin.murphy@mail.cisa.dhs.gov](mailto:justin.murphy@mail.cisa.dhs.gov)**

