Creating the Coordinator Rules

JPCERT Coordination Center
Global CVD Project Lead
Tomo Ito

The speaker information

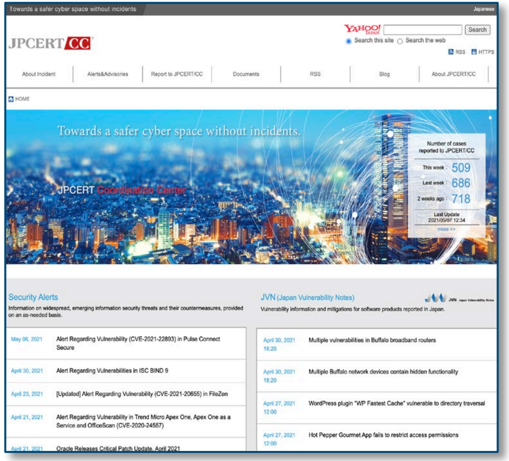
- JPCERT/CC Early Warning Group
  - CVD Coordinator
  - Global CVD Project Lead
    - CVD Harmonizing, International cooperation…

About JPCERT/CC

JPCERT/CC
Japan Computer Emergency Response Team
Coordination Center
JPCERT コーディネーションセンター

- Foundation: October 1996
- An independent (non-governmental), not-for-profit organization
  - Works for internet security
    - incident response
    - network monitoring
    - vulnerability coordination
    - ..
- Constituency: internet users in Japan

https://www.jpcert.or.jp/english/



Security Alerts

Information on widespread, emerging information security threats and their countermeasures, provided on an as-needed basis.

May 06, 2021	Alert Regarding Vulnerability (CVE-2021-22893) in Pulse Connect Secure
April 30, 2021	Alert Regarding Vulnerabilities in ISC BIND 9
April 23, 2021	[Updated] Alert Regarding Vulnerability (CVE-2021-20655) in FileZen
April 21, 2021	Alert Regarding Vulnerability in Trend Micro Apex One, Apex One as a Service and OfficeScan (CVE-2020-24557)
April 21, 2021	Oracle Releases Critical Patch Update, April 2021

JVN (Japan Vulnerability Notes)

Vulnerability information and mitigations for software products reported in Japan.

April 30, 2021 18:20	Multiple vulnerabilities in Buffalo broadband routers
April 30, 2021 18:20	Multiple Buffalo network devices contain hidden functionality
April 27, 2021 12:00	WordPress plugin "WP Fastest Cache" vulnerable to directory traversal
April 27, 2021 12:00	Hot Pepper Gourmet App fails to restrict access permissions

The background

CVD

Coordinated Vulnerability Disclosure

- ”Coordinated Vulnerability Disclosure (CVD) is the process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of software vulnerabilities and their mitigations to various stakeholders including the public. “

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330

Coordinated Vulnerability Disclosure

- ”Coordinated Vulnerability Disclosure (CVD) is the process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of software vulnerabilities and their mitigations to various stakeholders including the public. “

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330

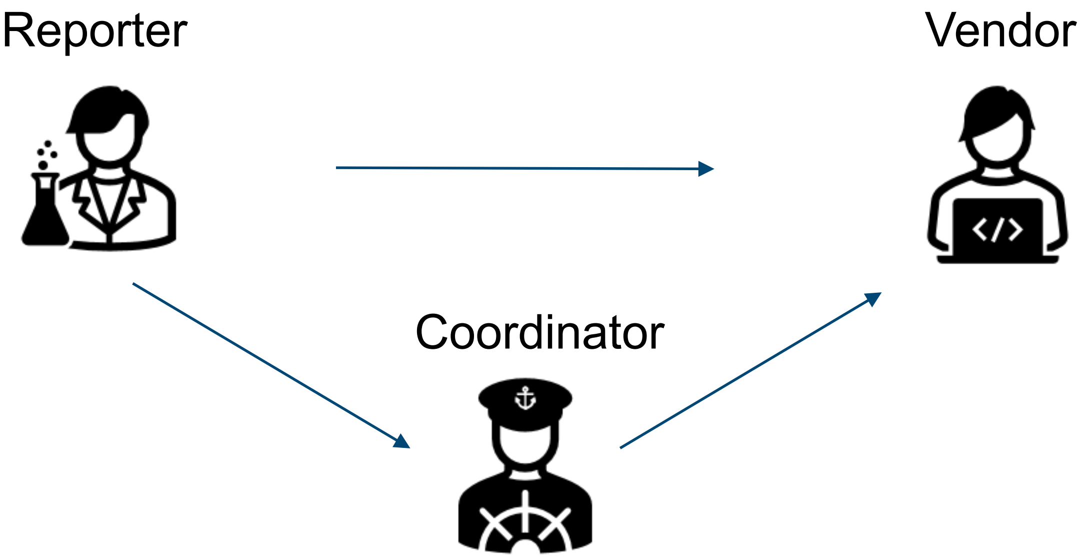
On CVD

- Important factors in CVD
  - Information is reached to appropriate stakeholders
  - Mitigation is created while vulnerability is undisclosed
  - Vul information is disclosed at an appropriate timing
  - Fix is applied
- The purpose of CVD is to reduce risks to the users, developers and the society

Global CVD/MPCVD happening

- Interdependent World
- CVD Stakeholders from around the globe
  - Reporters
  - Developers
  - Coordinators
  - Users
  - ….etc.

Single/Bi-lateral CVD Case



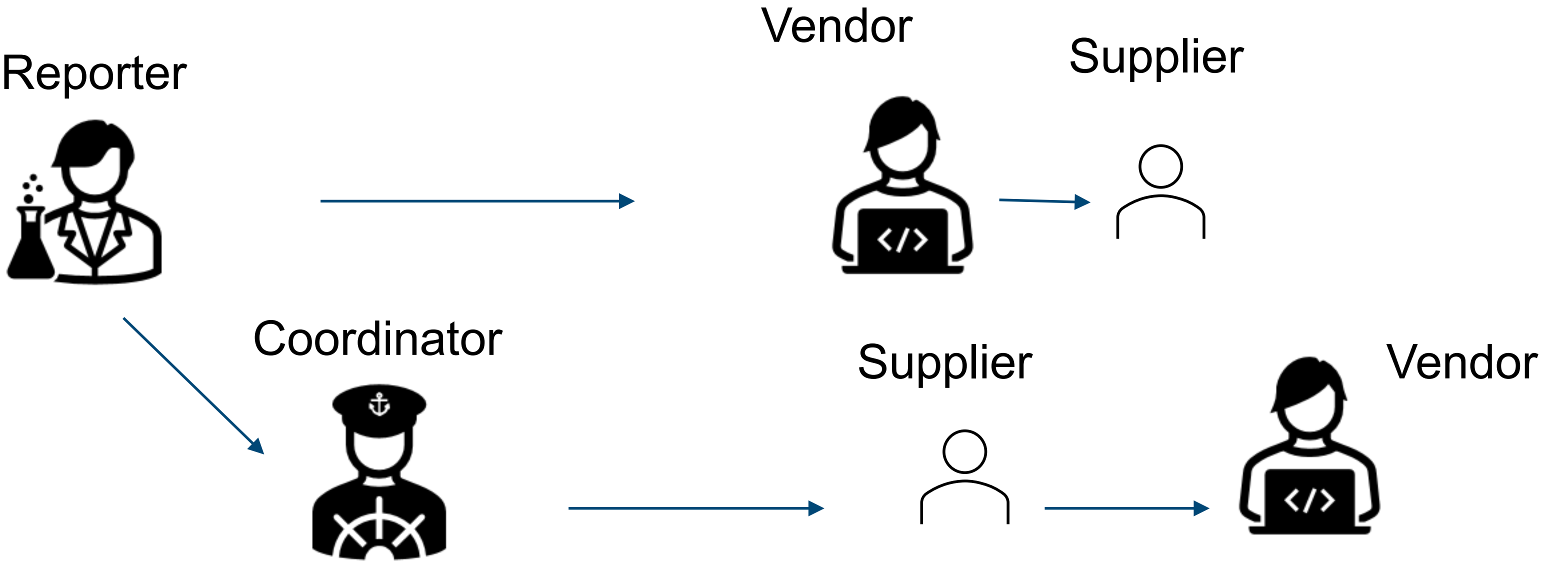
Reporter

Vendor

Coordinator

MPCVD – Complicated

- Multi-Party Coordinated Vulnerability Disclosure



CVD Coordinators

CVD Coordinators

- If CVD goes well between just reporters and developers
  - Totally Fine
- Still, Coordinators are often brought up/involved
  - Accept vulnerability reports
  - Notify appropriate stakeholders
  - Coordinate disclosure timings (especially in MPCVD)
  - Distribution of the publicly disclosed information
- Coordinators support CVD cases for the best outcomes

Image we had for the CVD players: Primarily..

- The CVD players' roles were thought to be more rigid and tied to the organizations or persons

Reporter

Coordinator

Vender

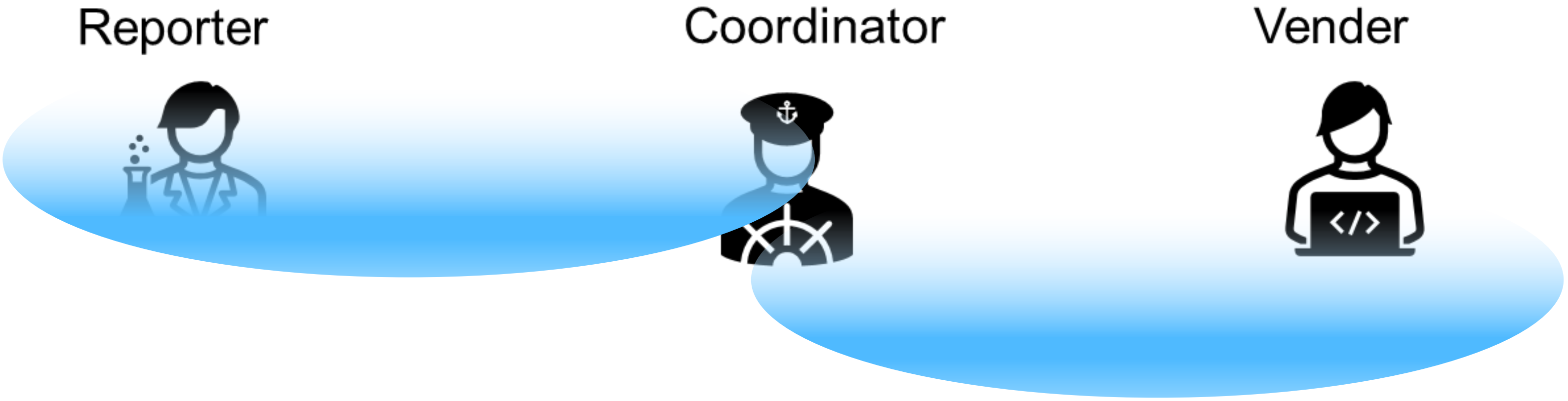
Reporters are supposed be doing such…

Coordinators are supposed be doing such…

Vendors are supposed be doing such…

Now & actually…

- Each roles often overlap - stakeholders often play multiple roles



Today…

- Multiple coordinator (like) organizations exist in the world

Each has its own mission/reasons/motivations of CVD

CERTs (“traditional” coordinators)

- improving the security of computer systems/networks within its scope..

Governments

- protecting the country’s citizens and infrastructures..

Bug bounty services

- protecting the product customers broadly, researcher encouragement..

Vendors

- protecting the users

- Intentionally or not, “coordinators” are all contributing to the social risk reduction and stability (if things go well in CVD)
- Processes may be similar, but the goals are often different

Coordinator confusions

CVD Coordinator confusions 1 – Lack of definition

- Coordinator Role has not been defined yet
  - What are the definitions, responsibilities, or capabilities of a Coordinator?
  - Reporters or developers often take the Coordinator role and coordinate
  - Different image for “coordinator” for each

<u>Expectations are unmatched in many cases</u>

CVD Coordinator confusions 2 – “foreign” issues

- There are many cases where developers are contacted by “foreign” coordinators suddenly
- CVD case fails/confusions occur from regional/cultural gaps
  - Language barriers
  - Cultural differences
  - Lack of mutual understandings

CVD Coordinator confusions 2

- Every coordinator is **LOCAL**
- Different organizations have different styles/goals
- Cultural differences are to be encouraged

..but imagine receiving a letter with a government name written on it with Japanese characters like **脆弱性調整** with some stamps on…

  - Hard to take appropriate actions

When their differences are too big, they cause confusions among the stakeholders and can cause CVD cases failures

Risks that occur from such confusions

- Unable to know what to expect from the coordinators
- Vulnerability information not reaching to the appropriate stakeholders
- Uncontrolled embargo timings
- Different skill levels between the coordinators
  - Too personalized
- Possibility of things becoming too “authoritative”

What to do?

- Coordinator role has not been defined
- In CVD, stakeholders other than Coordinators often act as a coordinator
- Too big of a difference between Coordinators cause confusions
- For more efficient global CVD activities

Why not define “Coordinator” & create rules?

From our interviews with the vendors

CVD Interviews with JP vendors

- JPCERT/CC conducted interviews with 6 different Japanese vendors on their global CVD situations
- All have experiences of receiving vulnerability reports from oversea coordinator organization(s) and conducting CVD with them
- The oversea coordinators are from the US, Netherlands, China, Germany & Switzerland

Excerpts from the interviews

Troubles in international CVD?

- Japan HQ unnotified of a CVD case
  - Case solved between the oversea branch & coordinator
  - HQ realized the issue when the advisory was published
- Hard to understand what the reporter is expecting
- Communications in different languages
- Lack of *coordination* in some cases ("too rough")
- Different thoughts for embargo timings
- Mutual understandings unsuccessful

…etc.

Additionally..

- 60% of the interviewees wishes JPCERT/CC involved in international CVD cases
- Miscommunication with the reporter
  - Both parties agreed it is “not a vulnerability” → The reporter spoke at a conference blaming the vendor for being insincere
- Lack of communication with the reporter as the government (coordinator) was in between

Speaking about the JP situations, but this can happen in other places – not asking to treat Japan special

Expectations unmatched

- Vulnerability reports from different coordinators from different parts of the world
- Troubles from cultural/regional gaps occurring
- Different laws/regulations are often concerned
- Voices of JPCERT/CC (Coordinator) involvement in CVD cases

Not blaming any parties/individuals

The Coordinator Rules

What to do

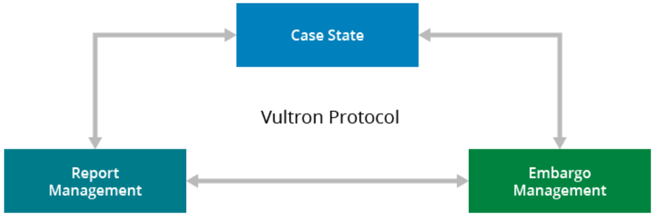
- Define Coordinator role
  - Other stakeholders such as reporters and vendors take the role
- Create basic set of rules
  - Like *global ethics* – no power over one another, no punishment
  - *Agreement* is the key

The rules should be in accordance with…

- FIRST Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure
- The CERT Guide to Coordinated Vulnerability Disclosure
- ISO/IEC 29147 Vulnerability disclosure
- ISO/IEC 30111 Vulnerability handling
- ISO/IEC TR 5895 Multi-party coordinated vulnerability disclosure

Also..

- There is Vultron Project by CERT/CC
  - CVD Protocol
  - Roles and states..
- The Coordinator Rules are to define "Coordinator (or "Coordination") to avoid mismatching in CVD processes



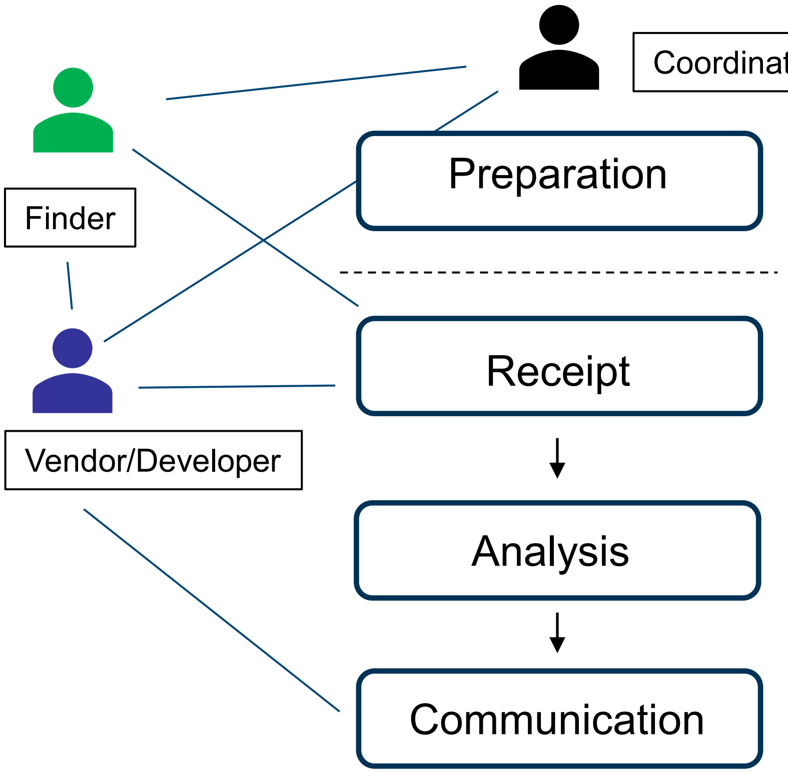
https://insights.sei.cmu.edu/blog/vultron-a-protocol-for-coordinated-vulnerability-disclosure/

An example (referencing ISO/IEC: 30111)

- Coordinator
  - General
  - Definition
  - Coordinator mission
  - Coordinator Responsibilities
  - Capabilities

- MPCVD Process
  - Preparation
  - Receipt
  - Analysis
  - Communication
    - Method
    - Choosing vendors (stakeholders)
    - Vendor registration
    - Information to be shared
  - Disclosing
    - Advisory format
    - What information to put

…etc.



The possible outcomes

- Global coordinators harmonization
  - Decrease unnecessary gaps
  - Enhance diversities
  - Match expectations within the stakeholders
  - Better cooperation
- Coordinator adoption
  - help for the starters
- Create coordinators' group..

Summary

- CVD role expectations between the stakeholders are often unmatched
- Value of CVD differs for different stakeholders
- “Coordinator” has not yet been defined
- Confusions regarding coordinators occurring due to regional/cultural/motivational differences
- It is necessary to define “Coordinator” and create rules/guidelines to avoid confusions

Opinions are always welcome

Tomo

- **Email：**tomotaka.itou@jpcert.or.jp

Thank you!