Sharing our CVD journey: Insights and lessons

JPCERT Coordination Center
Global Coordination Division, Director
Dr. Koichiro “Sparky” Komiyama

December 4, 2025, FIRST & AfricaCERT Symposium

Koichiro Komiyama

- Cyber security incident responder at JPCERT/CC
  - Director, Global Coordination Division
  - Leading the international engagement including capacity building program
- Former board member of FIRST.Org
- Scholar in Global Governance and Cyber Security policy
  - Ph.D. in Cyber security and International Relations
- www.sparky.jp for other publications

Geopolitics of Cyberspace. Released June 19, 2024.

My first visit to Mauritius, 2014

Key topic for This afternoon

- To protect our society, we must reduce the vulnerable software and hardware in the world. The process for achieving this is called Coordinated Vulnerability Disclosure, or CVD.
- The Africa also needs to strengthen its engagement in CVD.

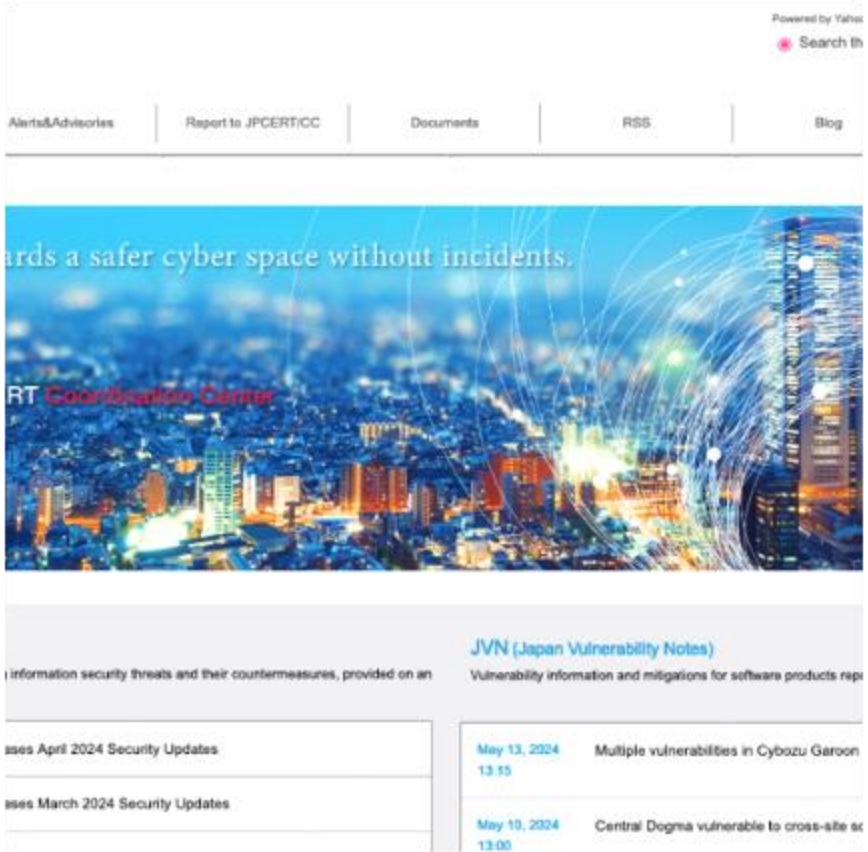
About JPCERT/CC

JPCERT Coordination Center

- A CERT (Computer Emergency Response Team)/CSIRT (Computer Security Incident Response Team) in Japan
- A non-profit, non-governmental, and independent organization
- The first CSIRT in Japan with 20+ years of experience (Founded in October 1996)

JPCERT/CC Activities

- Incident Handling
- Information Gathering/Analysis/Sharing
- Internet Traffic Monitoring
- Vulnerability Coordination
- Global Coordination
- Domestic Coordination
- …



CVD

Coordinated Vulnerability Disclosure (CVD)

- "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. "

The CERT Guide to Coordinated Vulnerability Disclosure
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330

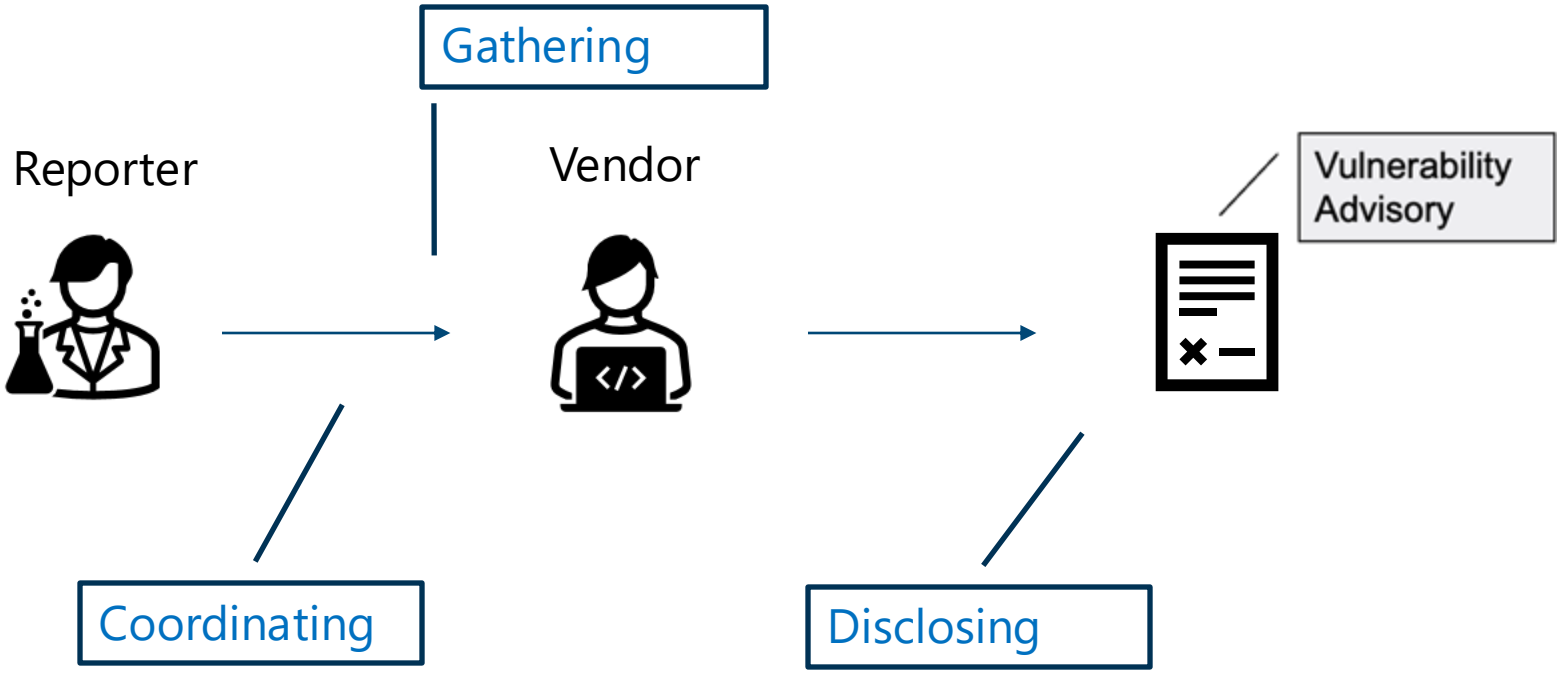
Coordinated Vulnerability Disclosure (CVD)

- Coordinated Vulnerability Disclosure (CVD)
  - It is a global good practice
  - Vulnerability information flows through global product supply chain
- The importance of CVD increasing
  - Attackers exploit vulnerabilities faster than ever
  - Regulatory pressure and global standards are expanding, impactful EU's Cyber Resilience Act.

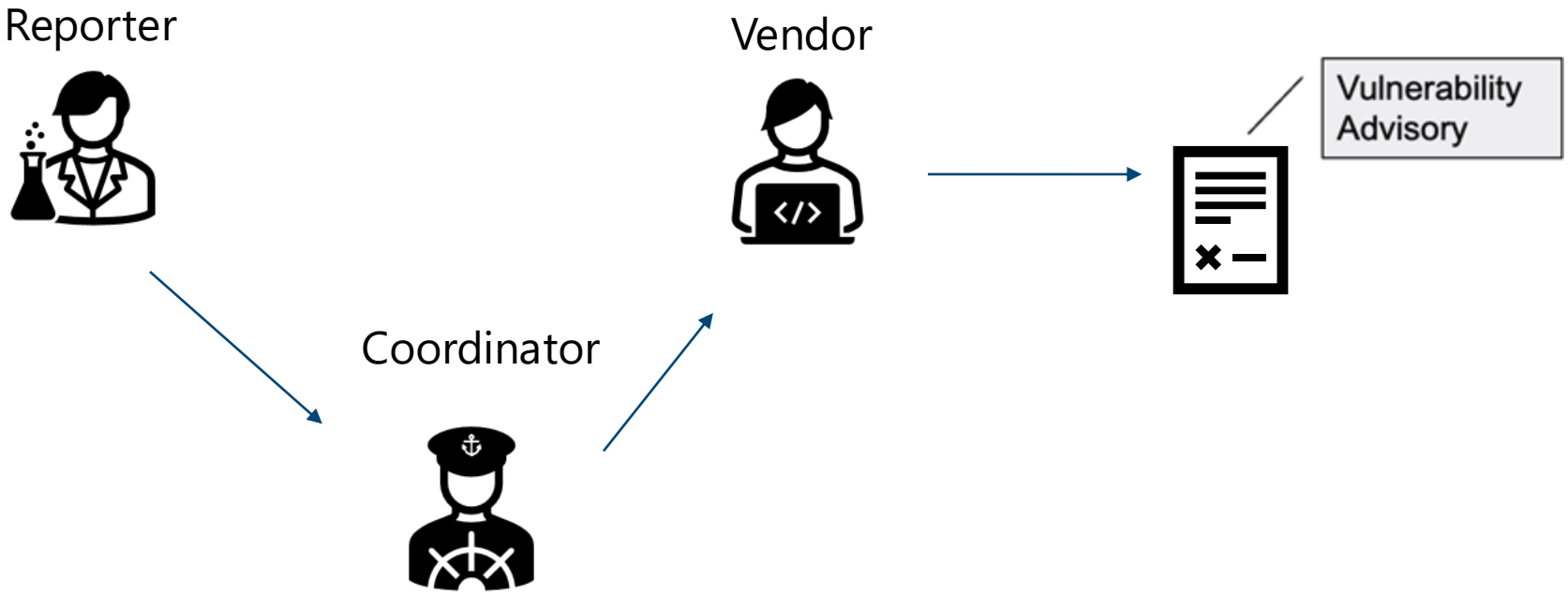
CVD Basic Stakeholders

- Reporter
  - Reports vulnerabilities
- Vendor
  - Vendor of the affected product, product owner
  - Fixes vulnerabilities
  - Publish vulnerability advisories
- User
  - User of the product
  - Affected by vulnerabilities
- Coordinator
  - 3rd party coordinator for CVD
  - “CVD Supporter” Acts as a mediator, provides opinion, often lead CVD cases
  - CERTs, Government agencies, etc.

CVD Basic information flow



Often Coordinators get involved



CVD Basic Processes

- Receipt
  - Receive vulnerability reports
  - Email, Web forms, etc.
- Verification & Triage
  - Vulnerability determination
  - Prioritize
- Coordination
  - Negotiate fix, advisory contents, disclosure dates
- …Disclosure
  - Publish vulnerability information as an advisory
  - Assign CVE, CWE, CVSS

The important factors and “Why CVD”

- Important factors of CVD
  - Information is reached to appropriate stakeholders
  - Mitigation is created before vulnerability is disclosed
  - Vul information is disclosed at an appropriate timing
  - Fix is applied
- Above not conducted = CVD case failure
  - May lead to zero-day, exploitation
- **The purpose of CVD is to reduce risks to the users, developers and the society**

CVD is global

Global CVD happening

- We live in an interdependent world
- Software components come from different parts of the world
- CVD is a global good practice
- Vulnerability information flows through global product supply chain
- CVD cases often fail due to cultural gaps/language barriers
  - Cooperation/Collaboration is a must

Challenge: Overcoming the gaps

- Cultural gaps/language barriers can lead to CVD cases failure
- More-region-specific CVD: Just make things harder
- Different situation and "CVD" for different stakeholders around the globe

Sharing JPCERT’s CVD journey

JPCERT/CC Vulnerability Coordination

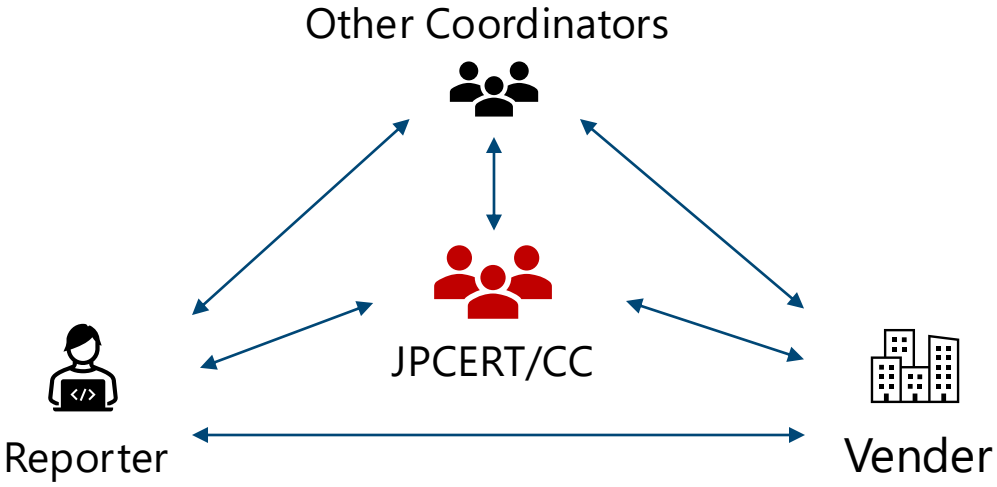
- JPCERT/CC acts globally as a CVD coordinator
  - Cooperate closely with domestic vendors who struggle with language/cultural differences to collaborate with overseas entities
    - Coordination with vendors: 1300+
      - Approx. ratio is Japan 65%: Overseas 35%
  - Assign CVEs to vulnerabilities coordinated by JPCERT/CC
  - Publish advisories on vulnerability information portal site “JVN”
  - Promote CVD
    - Document and training for Japanese Venders.

CNA and Root

- CNA since 2010 and Root since around 2017
  - promoting CNA activities in Japan by conducting material localization, recruiting, and online meetings to invite more organizations working as CNAs.
  - https://www.cve.org/PartnerInformation/ListofPartners/partner/jpcert
- Scope
  - Root: Japan organizations
  - CNA: Vulnerability assignment related to its vulnerability coordination role
- CVE assigned/published in 2024:
  - 276
- CNAs under JPCERT/CC Root
  - 10 organizations

JPCERT/CC CVD

- Primarily communicate by email
  - Also, a portal is available for exchanging of sensitive information
- Coordinate neutrally between different stakeholders



Vulnerability Handling Framework in Japan

- In Japan, vulnerability handling activities are specified in "Information Security Early Warning Partnership"
  - Created in accordance with the notification No. 235 issued in 2004 by the Ministry of Economy, Trade and Industry (METI)
  - JPCERT/CC is assigned as the vulnerability Coordinator
  - Reports received by Information-technology Promotion Agency (IPA)
  - Handle domestic/foreign products' vulnerabilities
  - Domestic vendors are "registered" in the framework

JPCERT/CC & JVN Timeline

- 2003: JVN started out as a research project
- 2004: JPCERT/CC designated as the Coordinator for Information Security Early Warning Partnership
- 2008: JVN English version launched
- 2010: JPCERT/CC became a CNA
- 2016: JPCERT/CC became a Root
- 2020: 2 CNAs under JPCERT/CC Root established
- 2025: More CNAs established and 10 CNAs under JPCERT/CC

1. Coordination

Coordination Challenges

- Different “CVD” for everyone
  - Differences in opinion
    - Whether to disclose the issue or not
    - How to proceed with the case
- Volume!
- Language barriers
  - Global CVD can be conducted between countries/regions of with different languages
  - Communication failure can lead to the CVD case failure

Sharing one experience

1. CERT requests MITRE for a CVE
2. No response from MITRE for a month
3. CERT is uncomfortable with the situation raised the issue to Japanese government
4. JPCERT/CC gets involved and asked to assign CVE
5. JPCERT/CC coordinate/raises issue at meetings, etc.

- Differences in opinion
  - There is no "absolute right" in this
  - But some stakeholders were upset
- Confusion
  - Government who is not close with CVE is involved
- Possibility of CVE duplicate
  - One CVE is being requested to MITRE but JPCERT/CC is later asked to assign one for the same issue

Important elements that can be learned from this case

- Respond in timely manner
- Patience
- Knowing who to talk to
- Promoting who should be talked to
- More communication
- Understanding the CVE processes more
- …etc.

Stakeholder engagement

Stakeholder engagement

- You deal with both domestic/foreign stakeholders in CVD
- You conduct CVD with stakeholders
  - Without reporters no vulnerability information is reported
  - Without vendors acting properly, no fixes are provided
  - Without Coordinators working together there could be regions which is left out out from an important CVD case
- Being engaged and cooperating with stakeholders is essential to keep your CVD Program moving forward
- Awareness: Explaining/understanding together of CVD is also essential

To achieve more smooth/efficient CVD…

- POC Meeting
  - Presentations by participants
  - Strengthen relationships with vendors
- Assist vendors' improvement
  - PSIRT training
  - Vulnerability coordination guide
  - Publish CWEs in Japanese on GitHub
- "Best Reporter Award" to encourage their activities
- Engage with global partners
  - At conferences, meetings
  - Collect and share international information
- CVD related WGs
  - APCERT CVD WG, CVD-COP

For the starters: Where to start?

To start CVD…

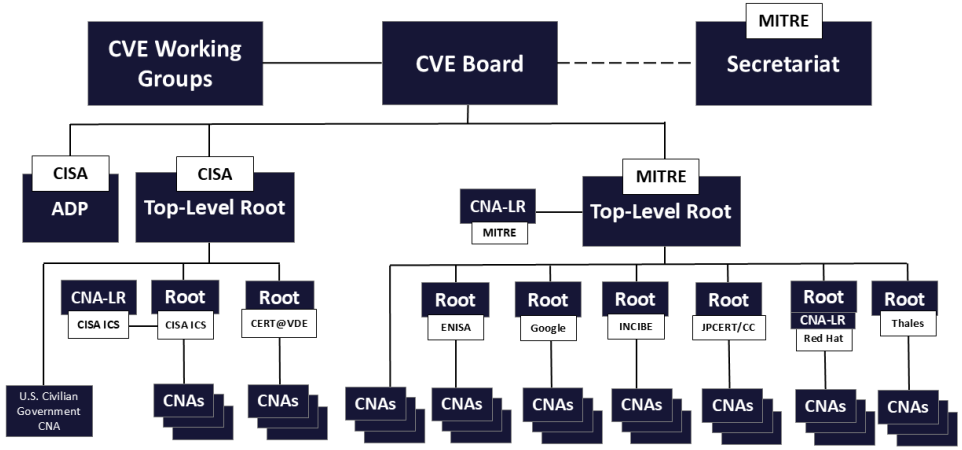
- Basic mechanisms you would need first are:
  - For receiving vulnerability reports: Vulnerability Disclosure Policy (VDP), Public point of contact
  - For coordination: Ticketing/communication system
  - For disclosure: Advisory location
- From these, we will touch a bit on VDP, as we often receive advice on this

Vulnerability Disclosure Policy (VDP)

- VDP is a set of rules that explain how vulnerability can be reported
- Vulnerability Disclosure Policy can include items such as:
  - Policy
  - Scope
  - Processes
  - Communication channels
  - How issues will be triaged
  - Embargo period
  - Disclosure

You can consider becoming a CNA

- To become a CNA, you must prepare:
  - Vulnerability Disclosure Policy
  - Public facing Point-of-Contact
  - Advisory location
- Becoming a CNA can help you with your CVD readiness
  - 8 different CNAs
  - Shop Beat Solutions (Pty) LTD (South Africa)



Resources

Resources 1

- The CERT Guide to Coordinated Vulnerability Disclosure
  - https://www.sei.cmu.edu/documents/1945/2017_003_001_503340.pdf
  - CVD Guide by CERT/CC
  - Useful information regarding CVD

- ISO/IEC 29147 (Vulnerability Disclosure) & 30111 (Vulnerability Handling)
  - 2 standards for CVD related activities

- Information Security Early Warning Partnership
  - https://www.ipa.go.jp/en/security/vulnerabilities/partnership.html
  - Explains the Japanese CVD framework, recommended actions, etc.

Resources 2

- Coordinated Vulnerability Disclosure Policies in the EU
  - https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu
  - 2022 document on EU member states' CVD situations
  - Also explains other information such as CVD policy good practices and challenges

- Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies
  - https://ec.europa.eu/newsroom/dae/redirection/document/99973
  - ENISA document on VDP
  - More for national or government organizations

Summary, Tips & Advice

Summary

- CVD is a global Good Practice
- Vulnerability information flows through global supply chain
- Different situation "CVD" for different parts of the world
- Importance of CVD increasing globally: Africa/Arab region is no exception
- Engagement & collaboration important in CVD

Tips & Advice

- Set your CVD policy in accordance with your situation
- Communication is the key
  - CVD cases can fail due to communication failure
  - Listen to what the stakeholders are saying
  - Be consistent and obtain trust through communication
- Engage/cooperate with stakeholders
  - Join working groups, industry groups, etc.
  - Hold/host meetings with different stakeholders
  - Share knowledge & experiences
- Differences are to be encouraged and respected, at the same time try to harmonize
  - CVD is global

Q & A

Thank you!

global-cc@jpcert.or.jp