CVD & CVE Introduction

JPCERT Coordination Center (JPCERT/CC)
Early Warning Group
Tomo Ito

About JPCERT/CC(1)

- Foundation: October 1996

  Japan Computer Emergency Response Team / Coordination Center

- An independent(non-governmental), not-for-profit organization
  - —Working for internet security
    - incident response
    - network monitoring
    - vulnerability coordination
    - ……..
- Constituency: internet users in Japan

About JPCERT/CC(1)

- Foundation: October 1996

  Japan Computer Emergency Response Team / Coordination Center
- An independent(non-governmental), not-for-profit organization
  - —Working for internet security
    - incident response
    - network monitoring
    - **vulnerability coordination**
    - ……..
- Constituency: internet users in Japan

CVD

CVD – What is it?

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

CVD – What is it?

”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. “

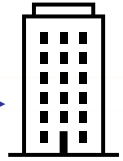
The CERT Guide to Coordinated Vulnerability Disclosure *Abstract*
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330

Why CVD?

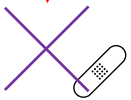
Researcher finds a vulnerability

Researcher/finder

Vul information is reported to appropriate stakeholders

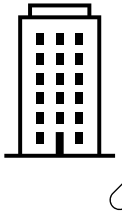


Coordinator



Vul information is sold to black market

Vul information published without mitigation



Vendor

Supplier

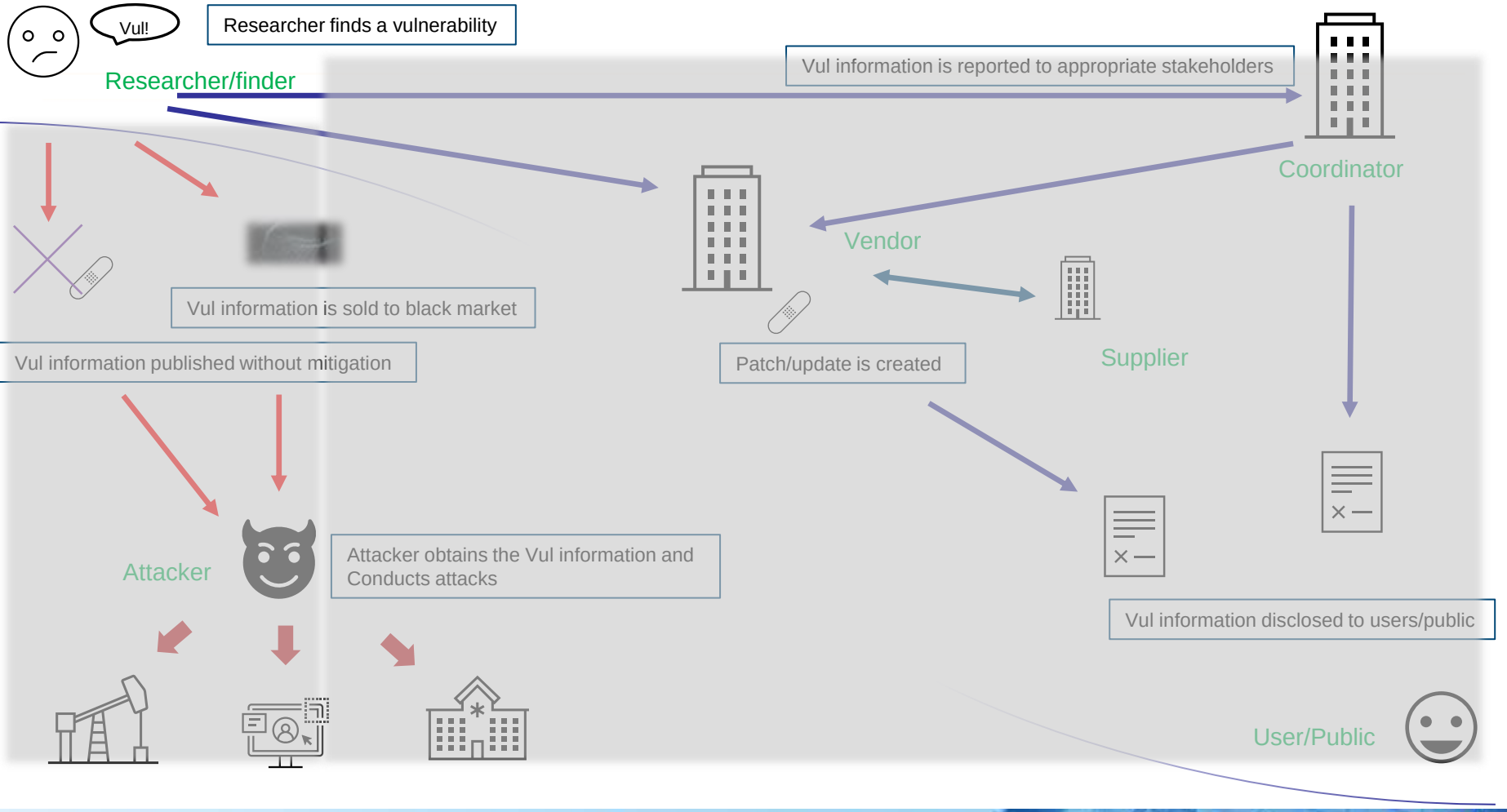
Patch/update is created

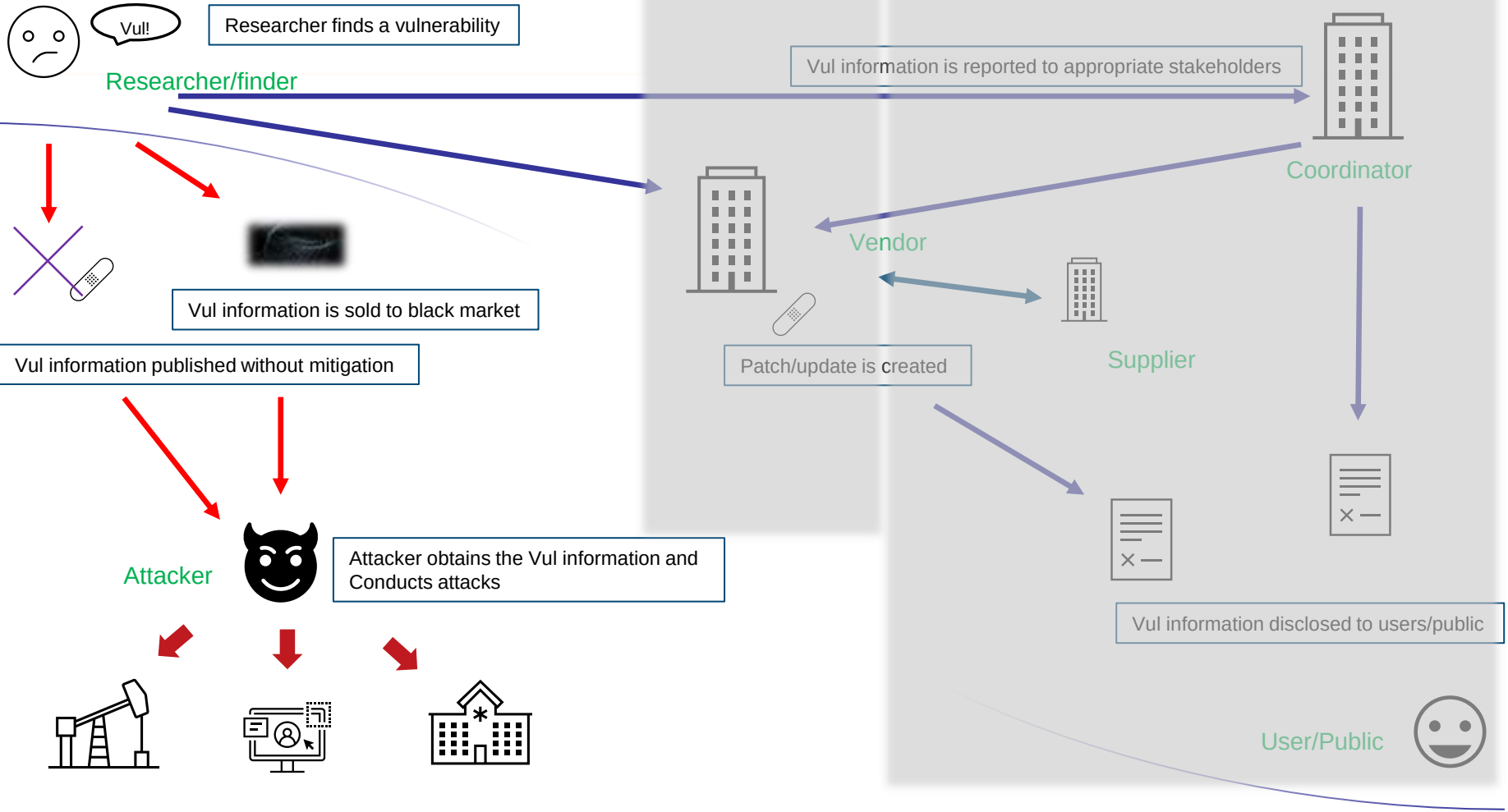
Attacker

Attacker obtains the Vul information and Conducts attacks

Vul information disclosed to users/public

User/Public





Researcher finds a vulnerability

Researcher/finder

Vul information is reported to appropriate stakeholders

Coordinator

Vendor

Supplier

Patch/update is created

Vul information is sold to black market

Vul information published without mitigation

Attacker

Attacker obtains the Vul information and Conducts attacks

Vul information disclosed to users/public

User/Public

Vulnerabilities are exploited in the wild

https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

- Pre-authentication remote code execution (RCE) vulnerability chain
- Reported on 2021-01-05, but in-the-wild exploitation had already started prior on 2021-01-03

Various costs resulting from vulnerabilities

- Cost for Developers
  - —product design review
  - —development and distribution of security updates
  - —customer support
  - —media support
  - —impact on stock price
- Cost for Users
  - —applying updates
  - —responding to attacks
  - —security measures
- Cost for Society
  - —attacks to critical infrastructures
  - —impact on supply chain

They need to be gathered, coordinated, and disclosed properly

Why do we remediate vulnerabilities?

Vulnerabilities raise various risks to

- users
- vendors
- society

We want to reduce these risks

CVD 3 basic elements

- 1. Gathering
  - Must be able to receive Vul information, when found
  - Display contact information, policy..
- 2. Coordinating
  - Connect with the appropriate stakeholders
  - Communicate/negotiate for the fix, disclosure, etc..
- 3. Disclosing
  - When the time comes, let the users know
  - Coordination often continues after disclosure

JPCERT/CC CVD

- Vulnerability Coordination
  - Handling private reports and public information
  - Analysis
  - Coordination with vendors
    - and with other stakeholders when necessary
  - Publishing on JVN (https://jvn.jp/, https://jvn.jp/en/)
  - Assigning CVE, CWE, CVSS

JPCERT/CC Vulnerability Coordination and Disclosure Policy
(https://www.jpcert.or.jp/english/vh/2018/20180330-vulpolicy.pdf)

JVN (Japan Vulnerability Notes)

https://jvn.jp/en/

https://jvn.jp/en/jp/JVN29739718/

Global CVD Ecosystem still in development

- Many stakeholders are involved (mostly from the western world)

  Finding/Reporting
  - Researchers

  Gathering/Coordinating/Disclosing
  - Vendors/Developers
  - CERT organizations
  - Government organizations

  Providing service/platform
  - Bug bounty services

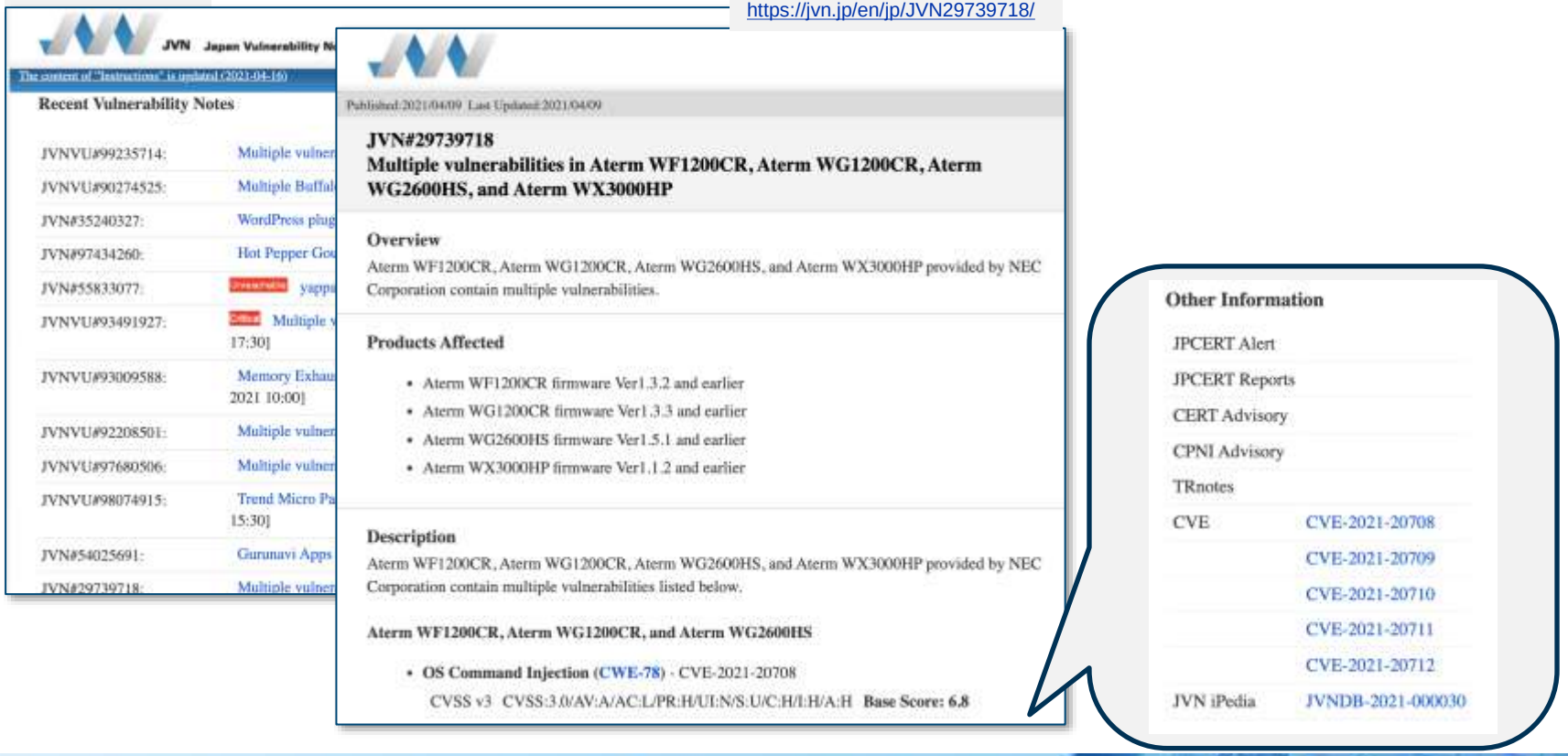
- Global cooperation is essential
  - components from several different parts of the world included in a product
  - more engagement from other regions needed

CVE – what connects the CVD stakeholders

JVN (Japan Vulnerability Notes)

https://jvn.jp/en/

https://jvn.jp/en/jp/JVN29739718/



Vulnerability identifier

- Identifies vulnerabilities
- Allows us to speak the same “language” and communicate
- Connection between the CVD stakeholders

Different orgs, different IDs

https://jvn.jp/vu/JVNVU94736763/

公開日：2020/06/18　最終更新日：2020/11/16

JVNVU#94736763
Treck 製 IP スタックに複数の脆弱性

概要
Treck 社が提供する IP スタックには複数の脆弱性が存在します。

CVE	CVE-2020-11896
	CVE-2020-11897
	CVE-2020-11898
	CVE-2020-11899
	CVE-2020-11900
	CVE-2020-11901
	CVE-2020-11902
	CVE-2020-11903
	CVE-2020-11904

https://kb.cert.org/vuls/id/257161

Home › Notes › VU#257161

Treck IP stacks contain multiple vulnerabilities

Vulnerability Note VU#257161

Original Release Date: [illegible] | Last Revised: 2021-03-17

Other Information

CVE IDs: CVE-2020-0594 CVE-2020-0595 CVE-2020-0597 CVE-2020-11896 CVE-2020-11897 CVE-2020-11898 CVE-2020-11899 CVE-2020-11900 CVE-2020-11901 CVE-2020-11902 CVE-2020-11903 CVE-2020-11904 CVE-2020-11905 CVE-2020-11906 CVE-2020-11907 CVE-2020-11908 CVE-2020-11909 CVE-2020-11910 CVE-2020-11911 CVE-2020-11912 CVE-2020-11913 CVE-2020-11914 CVE-2020-8674

CVE Program

- Mission:

”Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.”

- Founded in 1999
- Volunteer-based
- Currently 221 CNAs from Asia Pacific, Europe, North/South America, Middle East..

Australia: 2	Denmark: 1	Latvia: 1	South Korea: 4
Austria: 1	Estonia: 1	Netherlands: 4	Spain: 4
Belgium: 1	Finland: 3	New Zealand: 1	Sweden: 2
Canada: 5	France: 3	Norway: 1	Switzerland: 6
Chile: 1	Germany: 9	Romania: 1	Taiwan: 6
China: 9	India: 4	Russia: 2	Turkey: 3
Colombia: 1	Ireland: 1	Singapore: 1	UK: 6
Czech Republic: 1	Israel: 4	Slovak Republic: 1	USA: 117
	Japan: 8		Vietnam: 1

https://www.cve.org/ProgramOrganization/CNAs

CNA & Root

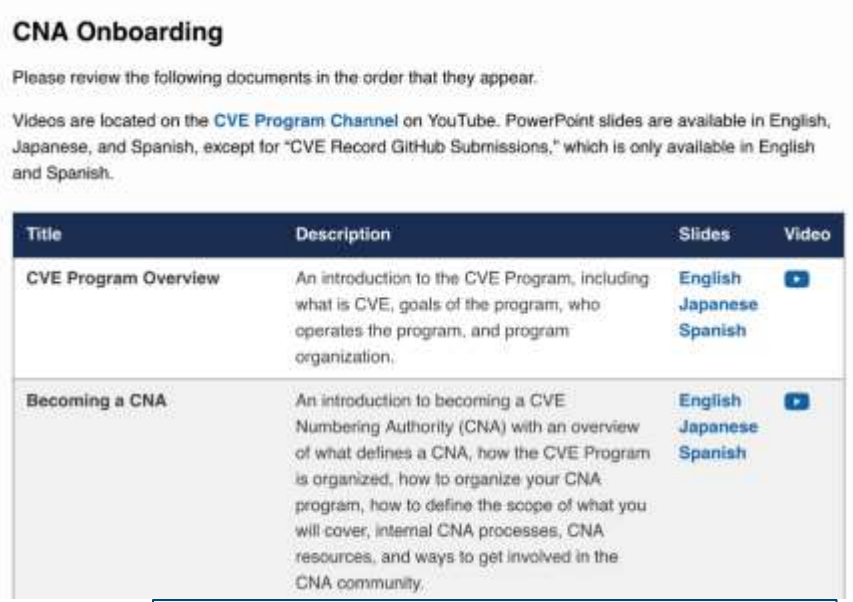
- CNA
  - Assigns CVE IDs (to vuls found within its scope)
  - To become a CNA, needs VDP, Advisory location, etc. prepared

A way to become CVD-ready

- Root
  - Recruits, creates, and manages CNAs
  - Currently 5 Roots
    (MITRE, CISA ICS, INCIBE, Google, and JPCERT/CC)

JPCERT/CC as a Root (1)

- CNA recruitments (prospects are found from our CVD activities)
- CVE handling training
- Material localization
- Holds conference “CNA Talk”, inviting scope CNAs.



CNA Onboarding

Please review the following documents in the order that they appear.

Videos are located on the CVE Program Channel on YouTube. PowerPoint slides are available in English, Japanese, and Spanish, except for “CVE Record GitHub Submissions,” which is only available in English and Spanish.

Title	Description	Slides	Video
CVE Program Overview	An introduction to the CVE Program, including what is CVE, goals of the program, who operates the program, and program organization.	English Japanese Spanish	
Becoming a CNA	An introduction to becoming a CVE Numbering Authority (CNA) with an overview of what defines a CNA, how the CVE Program is organized, how to organize your CNA program, how to define the scope of what you will cover, internal CNA processes, CNA resources, and ways to get involved in the CNA community.	English Japanese Spanish	

https://www.cve.org/ResourcesSupport/Resources#cnaOnboarding

JPCERT/CC as a Root (2)

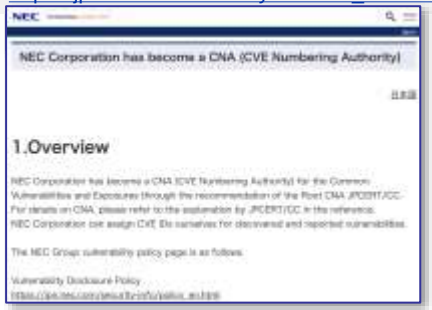
- CNAs
  - LINE, Mitsubishi, NEC, Toshiba, Panasonic

https://blogs.jpcert.or.jp/en/2020/12/cna-2cna.html

https://www.mitsubishielectric.com/en/psirt

https://linecorp.com/en/security/article/353

https://jpn.nec.com/security-info/cna_announce_en.html



https://holdings.panasonic/global/corporate/product-security/psirt/policy.html

(10) CVE Numbering Authority (CNA)

As of December 1, 2021, Panasonic PSIRT has become a CVE Numbering Authority (CNA). As a CNA, Panasonic PSIRT will assign CVE ID to vulnerabilities found in Panasonic products. For Panasonic products reported with vulnerabilities, we will assign CVE IDs and disclose them in a timely manner to protect the security and safety of our products and customers.

JPCERT/CC as a Root (3)

- JPCERT/CC Root scope
  - Currently ”Japan Organizations”
  - Expanding to Asia-Pacific region

Partner	Scope	Program Role	Organization Type	Country*
JPCERT/CC	**Root Scope:** Japan organizations **CNA Scope:** Vulnerability assignment related to its vulnerability coordination role	Root, CNA	National and Industry CERTs	Japan

https://www.cve.org/PartnerInformation/ListofPartners

Summary

Summary

- CVD is the process of reducing the risks to the users and the society
- 3 basic elements of CVD:
  - —Gathering, Coordinating, and Disclosing of Vulnerability information
- Components from many different countries/regions included in products – global engagement is essential
- We would like you to:
  - think what your CVD role is
  - know who your stakeholders are
  - consider becoming a CNA in the future
  - contact us if ***anything*** (questions, comments, …)

Contact

JPCERT/CC Early Warning Group
(Vulnerability Coordination)

- **Email : vuls@jpcert.or.jp**

tomotaka.itou@jpcert.or.jp

Thank you!