

# Vulnerability Handling in Japan and Linking through CVE

Takayuki (Taki) Uchiyama  
JPCERT Coordination Center, Japan  
November 14, 2012

- Vulnerability Handling Framework in Japan
- Global Linking of issues using CVE
- Q&A

- Vulnerability Handling Framework in Japan
- Global Linking of issues using CVE
- Q&A

## ■ Purpose:

- Process is designed to minimize the potential damage that a reported vulnerability may cause prior to public disclosure.

## ■ Simply Put:

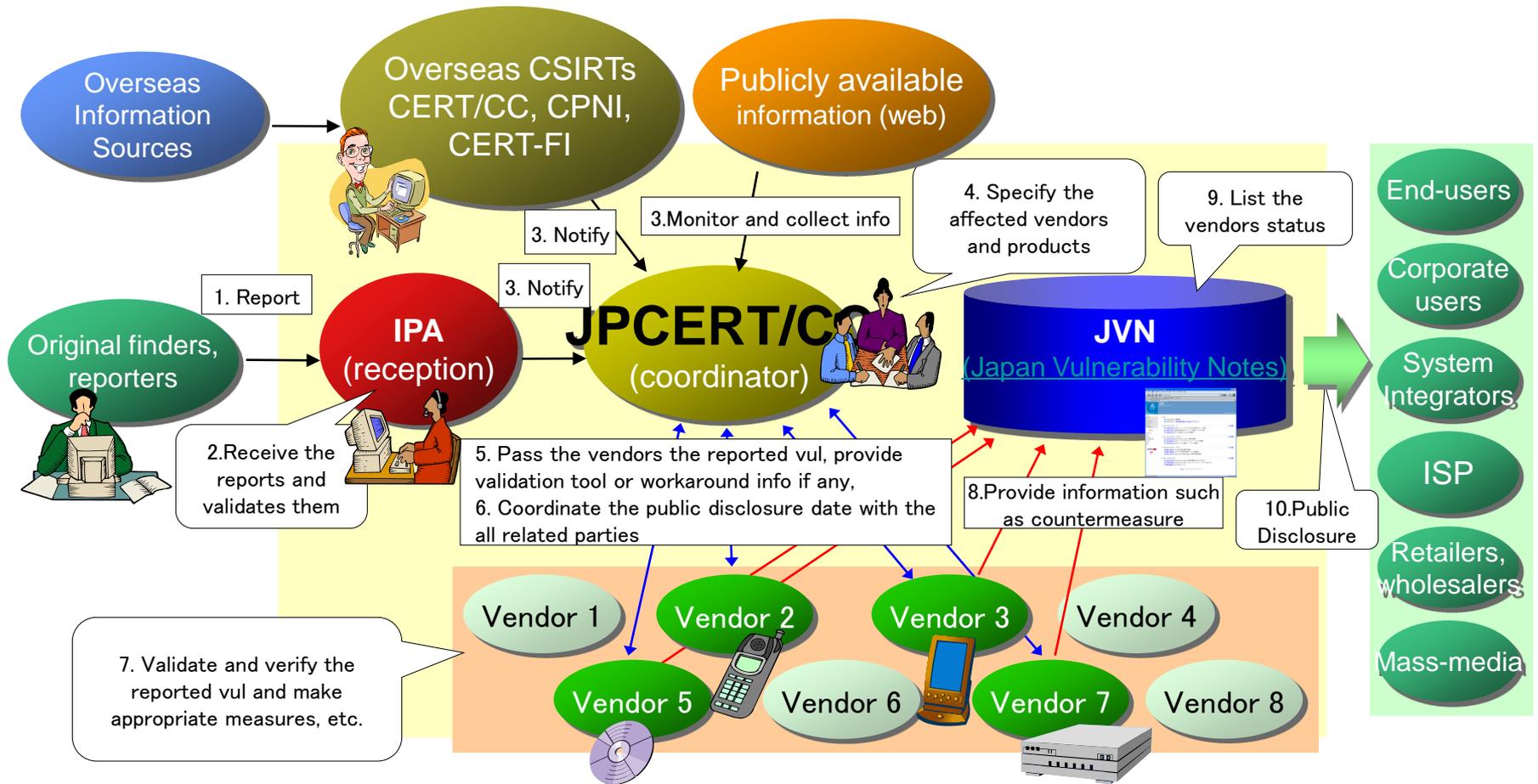
- Receive vulnerability report from the finder, report to the vendor, coordinate the release of the update/patch along with the vulnerability information
- More in detail a little later



## ■ Handling activities are governed by the “Notification of Ministry of Economy, Trade and Industry No. 235” issued in 2004

- In response to METI's notification, JPCERT/CC and IPA created the “Information Security Early Warning Partnership”
  - JPCERT/CC acts as the “Coordinator”
  - Coordinates handling activities with the developer
  
- All vulnerabilities reported within this framework are expected to be published on Japan Vulnerability Notes (JVN) – <https://jvn.jp/en/>
  - Issues are disclosed for the general public
  - Products that can be downloaded freely / vendors do not track users, etc.
  - There are some cases where the issue may not be published on JVN

# The Vulnerability Handling Process



### ■ Basic Steps for Vulnerability Handling in Japan:

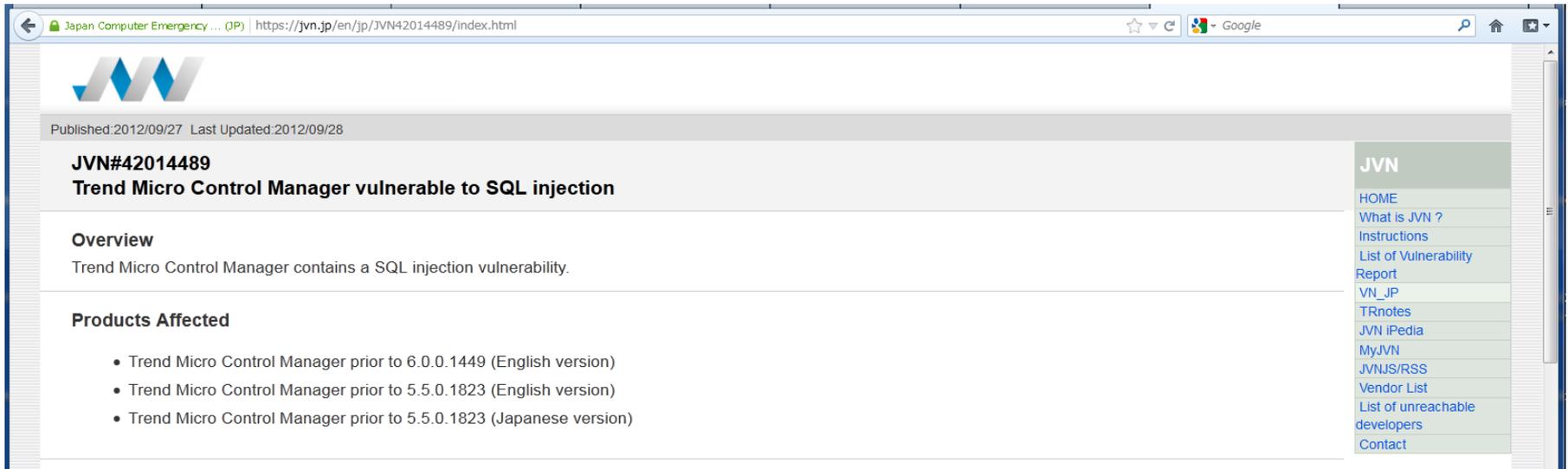
- Receive a vulnerability report (IPA)
- Analysis and reproduction of the reported vulnerability (IPA)
- Vendor Registration – First Contact (JPCERT/CC)
  - If JPCERT/CC has coordinated a vulnerability with the affected in the report, this step is skipped
- Vendor Coordination (JPCERT/CC)
  - If the vendor has any questions about the report, JPCERT/CC will contact IPA to contact the original reporter.
- Vendor Response (Vendor → JPCERT/CC)
  - Date for public release of update / patch / advisory occurs here
- Public Disclosure (Vendor, JPCERT/CC / IPA)
  - Disclosure on vendor site and JVN

- Unfortunately there are vendors that we cannot obtain contact with.
  - In these cases we cannot even report the vulnerability
  - No contact information on the website
  - Occurs more for OSS, but occasionally we have issues contacting vendors
  - Sometimes we obtain an email address but get no response
  - Since it may induce a 0-day, we do not send the report on the first contact
- Some vendors do not notify the status of the report
  - Working as the bridge to the reporter, would like to know the status to notify the Reporter
  - In some cases, when re-contacting a vendor, will be notified that they fixed a “while ago”

- In the 8+ years of the Information Security Early Warning Partnership, vendors have become more “willing” to coordinate vulnerabilities and disclose this information for its user base
  - Large vendors have led this for the most part
  
- Still hard to keep a stream of dialog with certain vendors / developers
  - Open source developers are much more inclined to keep dialog going and open to suggestions about a fix (in my personal experience)
  - Understandable since for vendors, products are a “business”

- There are issues that may potentially affect multiple vendors
  - Vulnerabilities in protocols or the implementation of a protocol
  - Vulnerabilities in a widely used library
    - Coordination is originally done with the library developer, but notification of the vulnerability may be done to vendors that use the library
  
- Some vendors may elect to coordinate only with the national CSIRT in their country
  - In these cases, JPCERT/CC will contact that CSIRT
  - Since 2011, some issues have been coordinated through KrCERT/CC (Korea) and CNCERT/CC (China)
  
- JPCERT/CC mainly coordinates with CERT/CC (US), CERT-FI (Finland), CPNI (UK) on issues that may affect multiple vendors

- As of the end of September 2012, a total of 1497 advisories have been released on JVN
  
- From the above, 667 advisories have been released as a result of the Japanese vulnerability handling framework
  - Issues that were originally reported in Japan or handled in the Japanese vulnerability framework have an English advisory on JVN
  
- The remaining advisories are part of global vulnerability handling,
  - Some issues are globally coordinated
  - Other issues are advisories that are localized to Japanese from the CERT/CC vulnerability note website



Japan Computer Emergency ... (JP) | https://jvn.jp/en/jp/JVN42014489/index.html

Published:2012/09/27 Last Updated:2012/09/28

## JVN#42014489

### Trend Micro Control Manager vulnerable to SQL injection

#### Overview

Trend Micro Control Manager contains a SQL injection vulnerability.

#### Products Affected

- Trend Micro Control Manager prior to 6.0.0.1449 (English version)
- Trend Micro Control Manager prior to 5.5.0.1823 (English version)
- Trend Micro Control Manager prior to 5.5.0.1823 (Japanese version)

#### JVN

- HOME
- What is JVN ?
- Instructions
- List of Vulnerability Report
- VN\_JP
- TRnotes
- JVN iPedia
- MyJVN
- JVNS/RSS
- Vendor List
- List of unreachable developers
- Contact

#### Other Information

JPCERT Alert

JPCERT Reports

CERT Advisory

CPNI Advisory

TRnotes

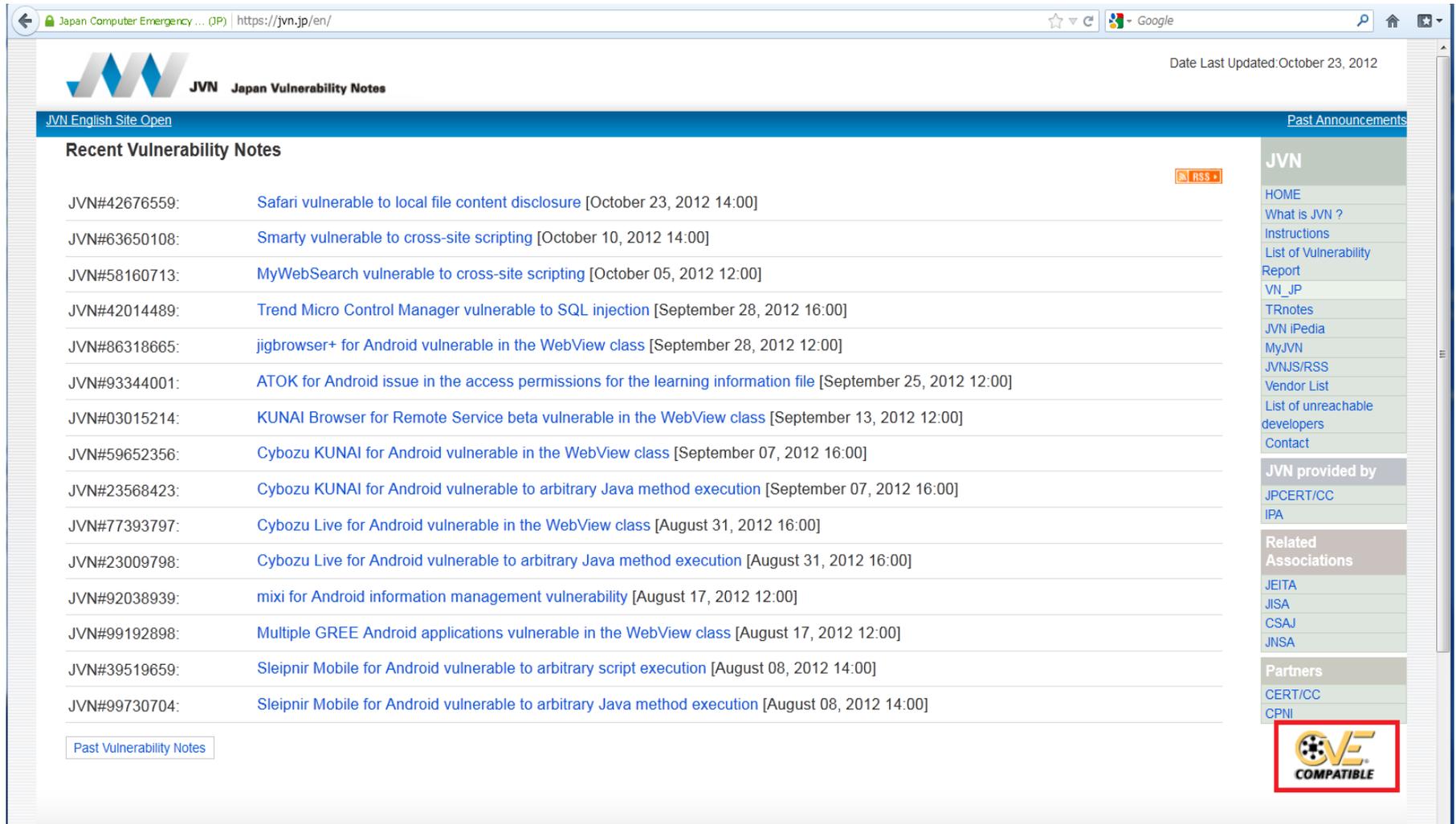
CVE [CVE-2012-2998](#)

JVN iPedia [JVNDB-2012-000090](#)

- Vulnerability Handling Framework in Japan
- **Global Linking of issues using CVE**
- Q&A

- Starting in 2008, JPCERT/CC acted as a reporter to have CVE's issued on vulnerabilities disclosed on JVN
  - This coordination occurred with MITRE
  
- On January of 2010, JVN became CVE compatible 
  
- As of March 2012, about 90% of reports on JVN contained a CVE identifier
  - What to do with reports that do not have CVE'S
  - On-going issue

# Screenshot of JVN English Site (with Logo)



The screenshot shows a web browser window displaying the JVN English site. The browser's address bar shows the URL <https://jvn.jp/en/>. The page header includes the JVN logo and the text "JVN Japan Vulnerability Notes". A navigation bar contains links for "JVN English Site Open" and "Past Announcements". The main content area is titled "Recent Vulnerability Notes" and features a list of 18 entries, each with a JVN ID, a title, and a date. An RSS feed icon is visible in the top right of this section. A sidebar on the right contains a "JVN" menu with links to HOME, What is JVN?, Instructions, List of Vulnerability Report, VN\_JP, TRnotes, JVN iPedia, MyJVN, JVNJS/RSS, Vendor List, List of unreachable developers, and Contact. Below this is a "JVN provided by" section listing JPCERT/CC and IPA. A "Related Associations" section lists JEITA, JISA, CSAJ, and JNSA. A "Partners" section lists CERT/CC and CPNI. At the bottom right of the sidebar is a logo for "VE COMPATIBLE".

Japan Computer Emergency ... (JP) | <https://jvn.jp/en/> | Google

Date Last Updated: October 23, 2012

**JVN Japan Vulnerability Notes**

[JVN English Site Open](#) [Past Announcements](#)

### Recent Vulnerability Notes

[RSS](#)

JVN#42676559:	<a href="#">Safari vulnerable to local file content disclosure</a> [October 23, 2012 14:00]
JVN#63650108:	<a href="#">Smarty vulnerable to cross-site scripting</a> [October 10, 2012 14:00]
JVN#58160713:	<a href="#">MyWebSearch vulnerable to cross-site scripting</a> [October 05, 2012 12:00]
JVN#42014489:	<a href="#">Trend Micro Control Manager vulnerable to SQL injection</a> [September 28, 2012 16:00]
JVN#86318665:	<a href="#">jigbrowser+ for Android vulnerable in the WebView class</a> [September 28, 2012 12:00]
JVN#93344001:	<a href="#">ATOK for Android issue in the access permissions for the learning information file</a> [September 25, 2012 12:00]
JVN#03015214:	<a href="#">KUNAI Browser for Remote Service beta vulnerable in the WebView class</a> [September 13, 2012 12:00]
JVN#59652356:	<a href="#">Cybozu KUNAI for Android vulnerable in the WebView class</a> [September 07, 2012 16:00]
JVN#23568423:	<a href="#">Cybozu KUNAI for Android vulnerable to arbitrary Java method execution</a> [September 07, 2012 16:00]
JVN#77393797:	<a href="#">Cybozu Live for Android vulnerable in the WebView class</a> [August 31, 2012 16:00]
JVN#23009798:	<a href="#">Cybozu Live for Android vulnerable to arbitrary Java method execution</a> [August 31, 2012 16:00]
JVN#92038939:	<a href="#">mixi for Android information management vulnerability</a> [August 17, 2012 12:00]
JVN#99192898:	<a href="#">Multiple GREE Android applications vulnerable in the WebView class</a> [August 17, 2012 12:00]
JVN#39519659:	<a href="#">Sleipnir Mobile for Android vulnerable to arbitrary script execution</a> [August 08, 2012 14:00]
JVN#99730704:	<a href="#">Sleipnir Mobile for Android vulnerable to arbitrary Java method execution</a> [August 08, 2012 14:00]

[Past Vulnerability Notes](#)

**JVN**

- HOME
- What is JVN ?
- Instructions
- List of Vulnerability Report
- VN\_JP
- TRnotes
- JVN iPedia
- MyJVN
- JVNJS/RSS
- Vendor List
- List of unreachable developers
- Contact

**JVN provided by**

- JPCERT/CC
- IPA

**Related Associations**

- JEITA
- JISA
- CSAJ
- JNSA

**Partners**

- CERT/CC
- CPNI



- As a result of our reporting activities, JPCERT/CC became a CVE Numbering Authority (CNA) in June 2010
  - JPCERT/CC has been assigning CVE' s for vulnerabilities released on JVN
  
- Vendor CNA issues are handled by the vendor
  - JPCERT/CC does not issue CVE' s for these issues
  - Some issues do not get assigned CVE' s
  - Receive CVE ID' s from the vendor for publication
  
- Depending on the issue JPCERT/CC will consult with MITRE to avoid duplication

Browser address bar: cve.mitre.org/cve/cna.html

Navigation: CVE LIST | COMPATIBILITY | NEWS — OCTOBER 1, 2012 | SEARCH

Logo: 

Common Vulnerabilities and Exposures  
*The Standard for Information Security Vulnerability Names*

TOTAL CVEs: 53138

HOME > CVE LIST > CVE NUMBERING AUTHORITIES

**About CVE**  
Terminology  
Documents  
FAQs

**CVE List**  
About CVE Identifiers  
Search CVE  
Search NVD  
Updates & RSS Feeds  
Request a CVE-ID

**CVE In Use**  
CVE-Compatible Products  
NVD for CVE Fix Information  
CVE Numbering Authorities

**News & Events**  
Calendar  
Free Newsletter

**Community**  
CVE Editorial Board  
Sponsor  
Contact Us

**Search the Site**

## CVE Numbering Authorities

[Introduction to CVE-ID Reservation](#) | [Role and Requirements of CNAs](#) | [Vendor Liaisons](#) | [Researcher Responsibilities](#) | [Requesting CVE-ID Numbers](#)

### Participating CNAs

The organizations below are participating as CVE Numbering Authorities (CNAs) as of October 2012:

#### Primary CNA

- MITRE Corporation ([cve-assign@mitre.org](mailto:cve-assign@mitre.org))

#### Software Vendors

- Apple Inc. (Apple issues only)
- Adobe Systems Incorporated (Adobe issues only)
- Hewlett-Packard Development Company, L.P. (H-P issues only)
- Oracle (Oracle issues only)
- Cisco Systems, Inc. (Cisco issues only)
- Red Hat, Inc. (Linux issues only)
- Debian GNU/Linux (Linux issues only)
- FreeBSD (primarily FreeBSD issues only)
- Ubuntu Linux (Linux issues only)
- Microsoft Corporation (Microsoft issues only)
- Silicon Graphics, Inc. (SGI issues only)
- EMC Corporation (EMC issues only)
- Novell/SUSE (Novell issues only)
- Google Inc. (Google issues only)
- IBM Corporation (IBM issues only)
- Research In Motion Limited (RIM issues only)

#### Third-Party Coordinators

- CERT/CC
- **JPCERT/CC**
- ICS-CERT

**CVE List**

- About CVE Identifiers
- Editorial Policies
- Data Sources
- Reference Key/Maps
- Search Tips
- Updates & RSS Feeds
- Request a CVE Identifier

**ITEMS OF INTEREST**

- Terminology
- NVD

- For issues that JPCERT/CC handles, JPCERT/CC typically assigns a CVE ID just prior to disclosure
  - This procedure may change if the developer / reporter requests a CVE prior to disclosure.
  - This process is taken just in case the developer obtains a CVE on their own.
    - The developer / researcher may contact a CNA that they know personally
    - This tends to occur more frequently in the Open Source community
  - JPCERT/CC attempts to synchronize JVN disclosures with vendor releases, but this can be very difficult.
    - A few hours is not a big deal, but one day, or even a weekend can not be avoided all the time

- Currently, JPCERT/CC checks the following prior to disclosure to avoid CVE duplication / collision
  - Vendor Site
  - CVE database
  - NVD
  - OSVDB (for open source products)
  - Others may be checked based on the situation
- Avoiding duplication / collision can only be done on a best effort basis
  - Sometimes we will consult MITRE prior to disclosure

- Handled a case where the reporter notified both CERT/CC and JPCERT/CC
  - CERT/CC was notified a few days earlier than JPCERT/CC
  - The English version of the product was released prior to the Japanese version
  - Coordination between JPCERT/CC and CERT/CC to release advisories when the Japanese version was ready
  - As a result, due to time difference, issue was disclosed on JVN first, followed by a release by CERT/CC
  - Since CERT/CC was notified prior to JPCERT/CC, and CERT/CC being a CNA, needed to check to see if CERT/CC had assigned a CVE ID
  - Since CERT/CC and JPCERT/CC coordination is a smooth process, we were able to obtain the CVE ID for this issue from CERT/CC via the reporter

## Issues with CVE assignment from the eyes of JPCERT/CC

- Vendors do not issue CVE identifiers for certain issues
  - Each vendor has their own policy on CVE assignment
  
- Older issues that may have been disclosed previously without a CVE are hard to trace
  - Somebody may or may not have issued a CVE in the past.
  - Can be difficult to avoid a “collision” or “duplicate” assigning in these cases
  
- Protocol / Library issues
  - Assign 1 CVE for the protocol, or
  - Assign a CVE for each vendor implementation
  - Which is better? The content decision questions can lead to 2 different conclusions

## ■ Architectural Issues

- Similar to protocol / library issues
- Ex. Windows DLL pre-loading issue
- Content decisions may lead to 2 different conclusions depending on the person applying the content decisions

- Vulnerability Handling Framework in Japan
- Global Linking of issues using CVE
- Q&A

# Thank you very much for your attention

General Inquiries:

Email: [office@jpcert.or.jp](mailto:office@jpcert.or.jp)

Tel: +81-3-3518-4600

Web: <https://www.jpcert.or.jp/english/>

Inquiries about Vulnerability Handling:

Email: [vultures@jpcert.or.jp](mailto:vultures@jpcert.or.jp)

Tel: +81-3-3518-4600

Web: <https://jvn.jp/en/>