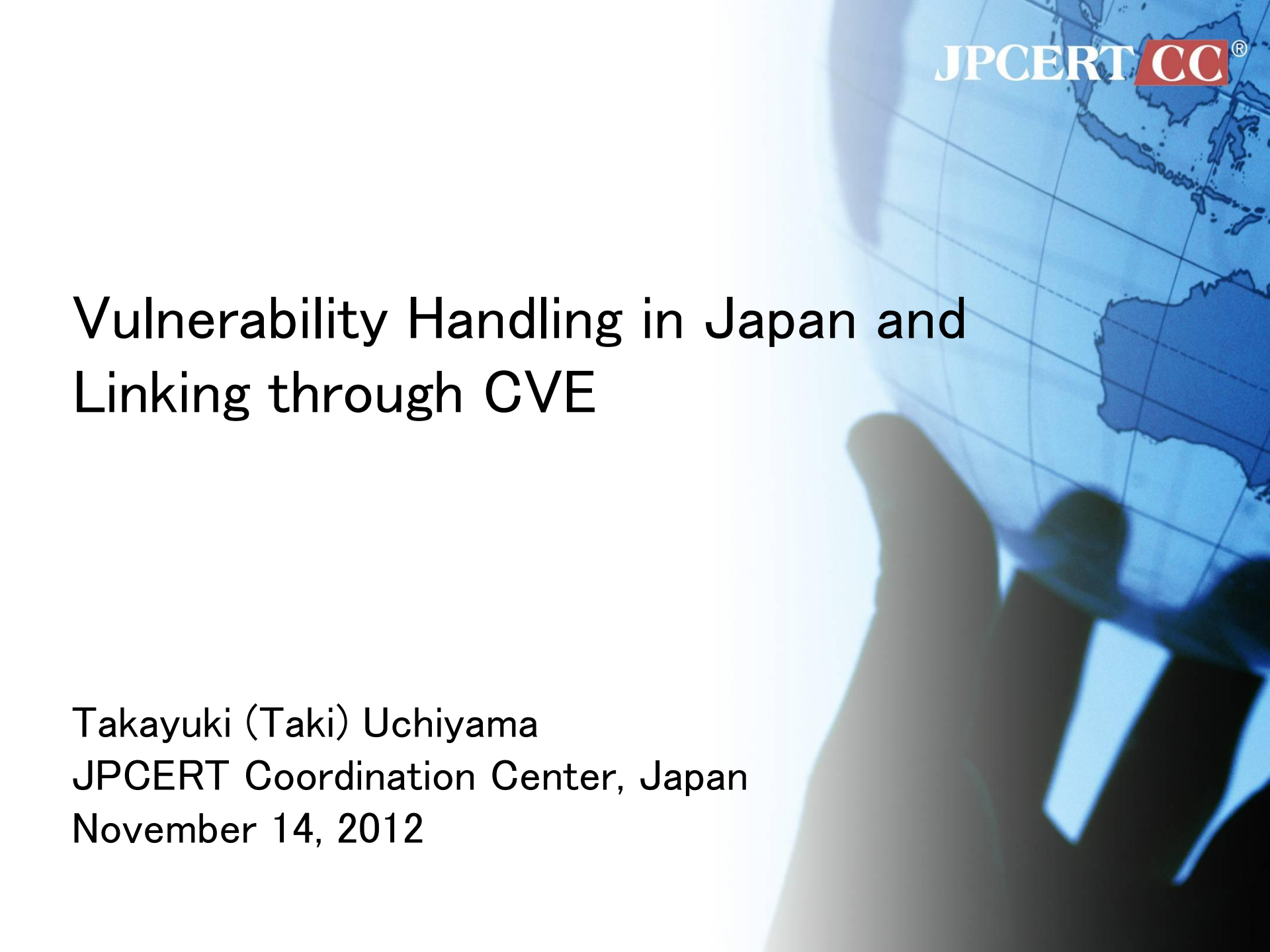


Vulnerability Handling in Japan and Linking through CVE

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

Agenda

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

Agenda

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

Vulnerability Handling Framework in Japan

JPCERT CC®

- 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

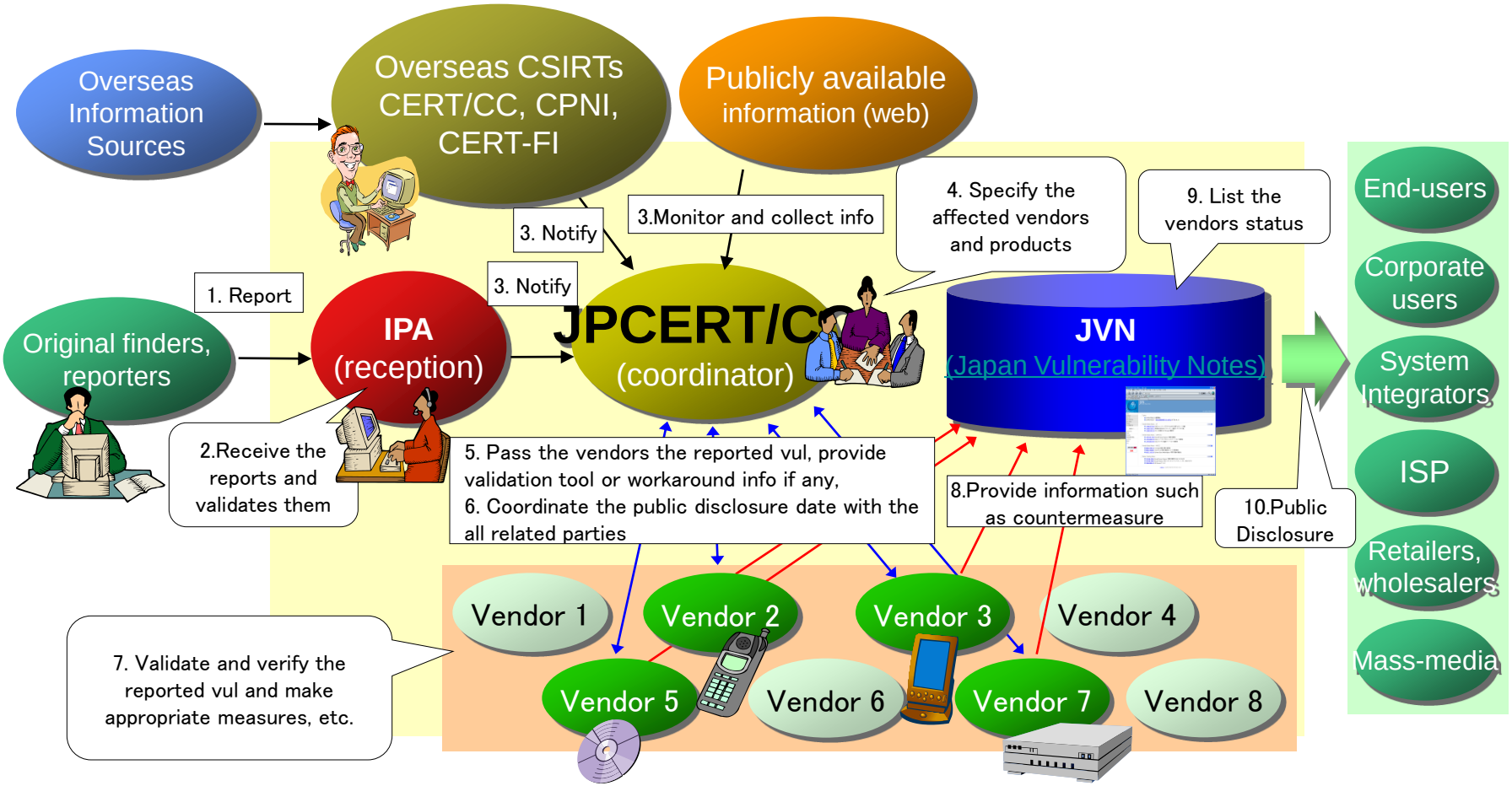
- Handling activities are governed by the “Notification of Ministry of Economy, Trade and Industry No. 235” issued in 2004

Vulnerability Handling Framework in Japan – 2

- 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  - There are some cases where the issue may not be published on JVN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



The Vulnerability Handling Process – 2

JPCERT CC®

- 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

Vendors that are hard to contact

- 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"

Vendors that are hard to contact – 2

- 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"

Global Vulnerability Handling

- 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

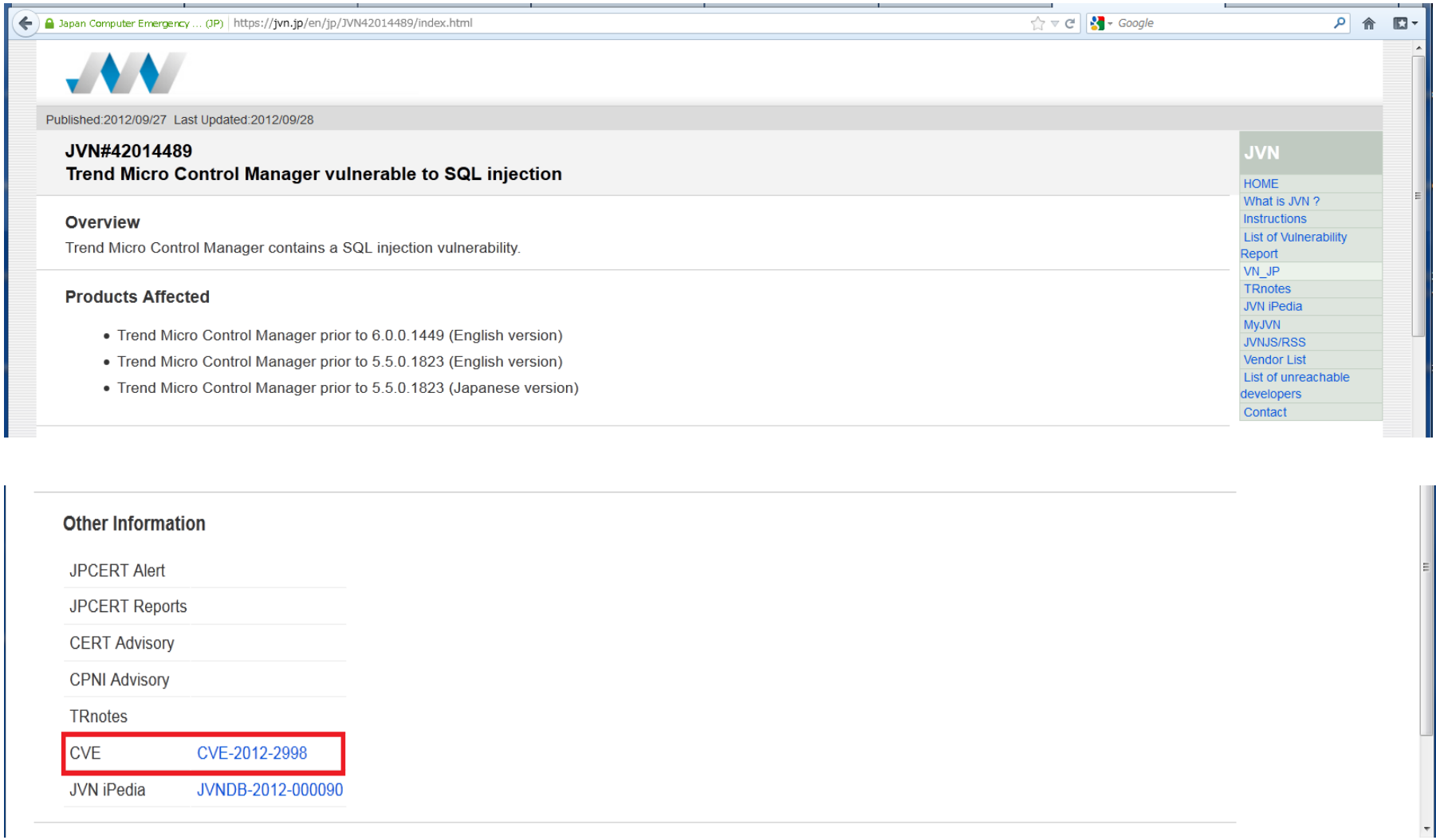
- Some vendors may elect to coordinate only with the national CSIRT in their country
  - In these cases, JPCERT/CC will contact that CSIRT
  - Since 2011, some issues have been coordinated through KrCERT/CC (Korea) and CNCERT/CC (China)

- JPCERT/CC mainly coordinates with CERT/CC (US), CERT-FI (Finland), CPNI (UK) on issues that may affect multiple vendors

JVN Advisories

- 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

JVN Advisory Screenshot



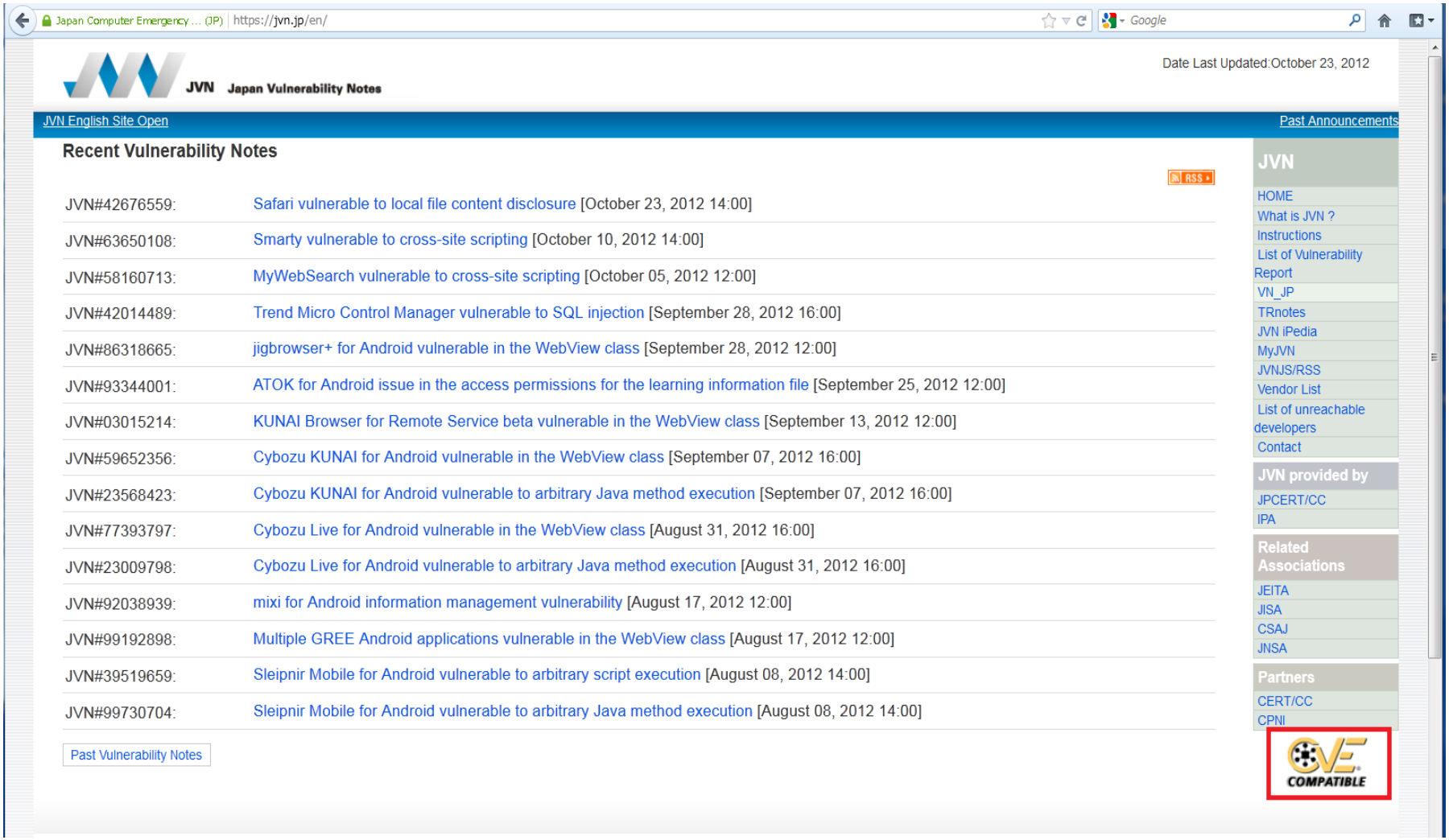
Agenda

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

JVN and CVE Compatibility

- 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

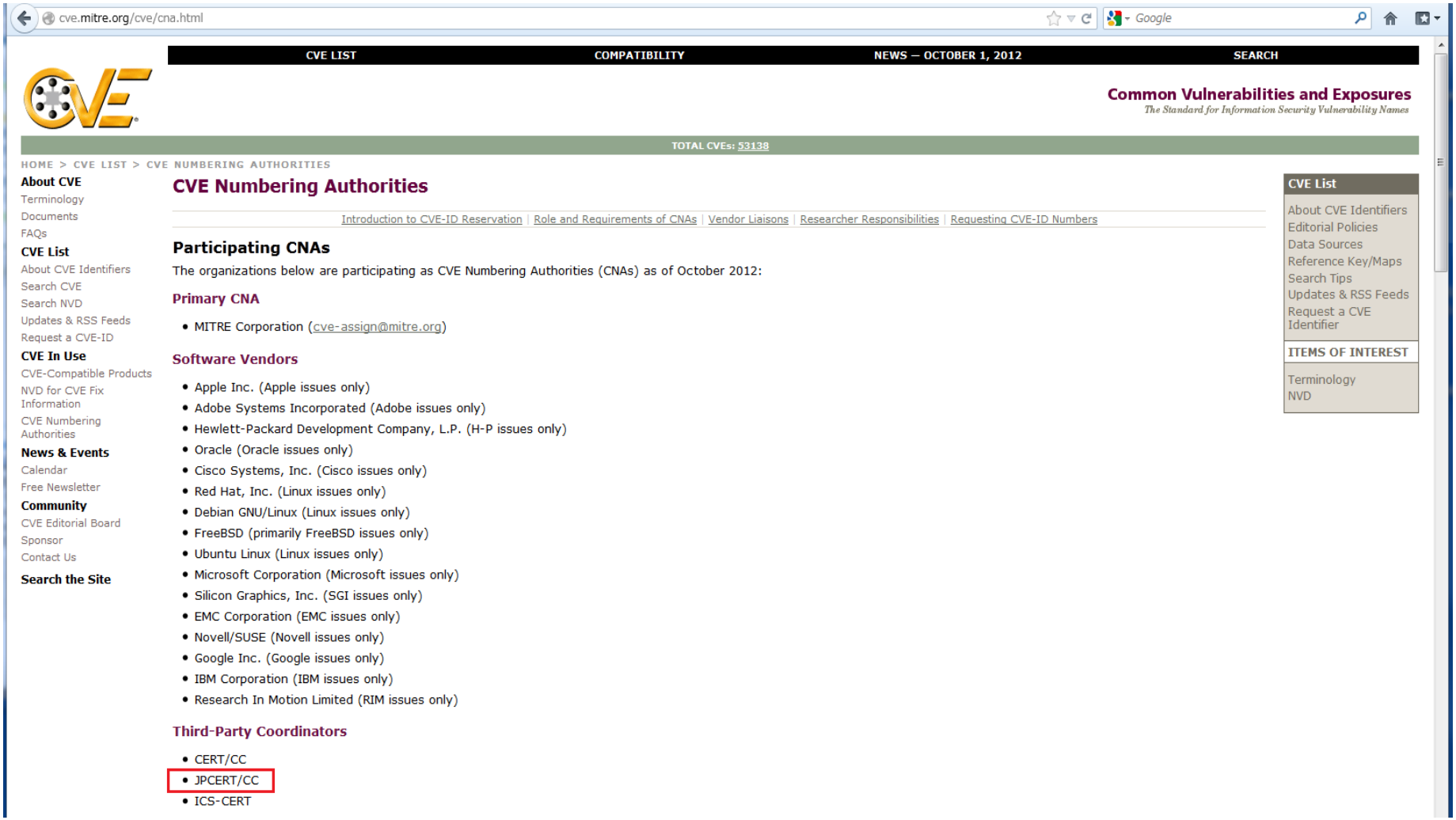
Screenshot of JVN English Site (with Logo)



JPCERT/CC as a CVE Numbering Authority (CNA)

- 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

CVE Numbering Authority



cve.mitre.org/cve/cna.html

CVE LIST | COMPATIBILITY | NEWS -- OCTOBER 1, 2012 | SEARCH

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)

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

JPCERT/CC CVE assignment and experiences

- 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

JPCERT/CC CVE assignment and experiences – 2

- 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

An example of Global Handling

- 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

Issues with CVE assignment from the eyes of JPCERT/CC – 2

- 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

Agenda

- 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
Tel : +81-3-3518-4600
Web: https://www.jpcert.or.jp/english/

Inquiries about Vulnerability Handling:
Email: vultures@jpcert.or.jp
Tel: +81-3-3518-4600
Web: https://jvn.jp/en/