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

- **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/](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- There are some cases where the issue may not be published on JVN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

1. Report
2. Receive the reports and validates them
3. Notify
4. Specify the affected vendors and products
5. Pass the vendors the reported vul, provide validation tool or workaround info if any
6. Coordinate the public disclosure date with the all related parties
7. Validate and verify the reported vul and make appropriate measures, etc.
8. Provide information such as countermeasure
9. List the vendors status
10. Public Disclosure

Overseas CSIRTs
CERT/CC, CPNI, CERT-FI
Publicly available information (web)

Original finders, reporters

IPA (reception)

JPCERT/CC (coordinator)

JVN (Japan Vulnerability Notes)

Vendor 1
Vendor 2
Vendor 3
Vendor 4
Vendor 5
Vendor 6
Vendor 7
Vendor 8

End-users
Corporate users
System Integrators
ISP
Retailers, wholesalers
Mass-media

Overseas Information Sources

End-users
Corporate users
System Integrators
ISP
Retailers, wholesalers
Mass-media

End-users
Corporate users
System Integrators
ISP
Retailers, wholesalers
Mass-media
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”
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
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

**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 5.5.0.1623 (English version)
- Trend Micro Control Manager prior to 5.5.0.1823 (Japanese version)

**Other Information**
- JPCERT Alert
- JPCERT Reports
- CERT Advisory
- CPNI Advisory
- TRnotes
- **CVE** CVE-2012-2998
- JVN iPedia JVNDB-2012-000090
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
## Recent Vulnerability Notes

<table>
<thead>
<tr>
<th>JVN#</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>JVN#42676559</td>
<td>Safari vulnerable to local file content disclosure</td>
<td>October 23, 2012 14:00</td>
</tr>
<tr>
<td>JVN#63650108</td>
<td>Smarty vulnerable to cross-site scripting</td>
<td>October 10, 2012 14:00</td>
</tr>
<tr>
<td>JVN#58160713</td>
<td>MyWebSearch vulnerable to cross-site scripting</td>
<td>October 05, 2012 12:00</td>
</tr>
<tr>
<td>JVN#42014489</td>
<td>Trend Micro Control Manager vulnerable to SQL injection</td>
<td>September 28, 2012 16:00</td>
</tr>
<tr>
<td>JVN#88318685</td>
<td>jgbrowser+ for Android vulnerable in the WebView class</td>
<td>September 28, 2012 12:00</td>
</tr>
<tr>
<td>JVN#93344001</td>
<td>ATOK for Android issue in the access permissions for the learning information file</td>
<td>September 25, 2012 12:00</td>
</tr>
<tr>
<td>JVN#03015214</td>
<td>KUNAI Browser for Remote Service beta vulnerable in the WebView class</td>
<td>September 13, 2012 12:00</td>
</tr>
<tr>
<td>JVN#56652356</td>
<td>Cybozu KUNAI for Android vulnerable in the WebView class</td>
<td>September 07, 2012 16:00</td>
</tr>
<tr>
<td>JVN#2356423</td>
<td>Cybozu KUNAI for Android vulnerable to arbitrary Java method execution</td>
<td>September 07, 2012 16:00</td>
</tr>
<tr>
<td>JVN#77393797</td>
<td>Cybozu Live for Android vulnerable in the WebView class</td>
<td>August 31, 2012 16:00</td>
</tr>
<tr>
<td>JVN#23009708</td>
<td>Cybozu Live for Android vulnerable to arbitrary Java method execution</td>
<td>August 31, 2012 16:00</td>
</tr>
<tr>
<td>JVN#920389700</td>
<td>mixi for Android information management vulnerability</td>
<td>August 17, 2012 12:00</td>
</tr>
<tr>
<td>JVN#99192898</td>
<td>Multiple GREE Android applications vulnerable in the WebView class</td>
<td>August 17, 2012 12:00</td>
</tr>
<tr>
<td>JVN#39519659</td>
<td>Sleipnir Mobile for Android vulnerable to arbitrary script execution</td>
<td>August 08, 2012 14:00</td>
</tr>
<tr>
<td>JVN#00730704</td>
<td>Sleipnir Mobile for Android vulnerable to arbitrary Java method execution</td>
<td>August 08, 2012 14:00</td>
</tr>
</tbody>
</table>

## Past Vulnerability Notes
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 Authorities

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
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
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/