Summit Days

Structure and numbering of JVN, and Security content automation framework

Masato Terada
IT Security Center, IPA

November 14, 2012
This session provides an overview of how JVN has adopted SCAP.

- JVN stands for "Japan Vulnerability Notes" and provides vulnerability and related information on software used in Japan.
- JVN has adopted SCAP, and provides local (domestic) information and international information, resulting in the JVN Security Content Automation Framework (MyJVN).
Structure and numbering of JVN
- JVN Security Content Automation Framework
- MyJVN project
structure and numbering of jvn.
= ( Internationalization + Localization ) x Machine readable

- **MyJVN**
  Providing vulnerability countermeasure information via machine readable interface such as Web APIs and Version Checker etc.

- **JVN (Vulnerability handling coordination DB)**
  Providing vulnerability countermeasure information and Japanese vendor status for reported vulnerabilities by “Information Security Early Warning Partnership”

- **JVN iPedia (Vulnerability archiving DB)**
  Providing countermeasure information database for covering overall vulnerabilities
structure and numbering of jvn.
Structure

- Flow of data exchange between DBs

Machine readable interface by Web APIs using CVE, CPE, CWE and CVSS.

JVN(JVN#12345678)
Vulnerability Handling Coordination DB

- Japanese Version
  http://jvn.jp/
- English Version
  http://jvn.jp/en/

Vulnerability Archiving DB

- Japanese Version
  http://jvndb.jvn.jp/
- English Version
  http://jvndb.jvn.jp/en/

Flow of data exchange between DBs:
- From CERT/CC, CPNI, CERT-Fl etc.
- From Information Security Early Warning Partnership in Japan (667)
- From CERT/CC, CPNI etc. (1,512)
- From Japanese software developers (135)
- From NVD (28,529)
- From Information Security Early Warning Partnership in Japan (667)

Translation

- NVD(English) (About 53,000)
- From JVN (2,179)
- From JVN (682)
- (Total 817)

Archiving

- Japanese software developers (135)
- Japanese software developers (135)
- 2012 3th Quarter
Assign three identifiers
- **JVN#12345678**
- **JVNDB-yyyy-123456**
- **CVE-yyyy-1234**

Assign two identifiers
- **JVNDB-yyyy-123456**
- **CVE-yyyy-1234**

---

Structure and numbering of JVN.

Numbering

---

Information Security Early Warning Partnership

CERT/CC
CPNI
CERT-FI etc.

Japanese software developers

NVD(English)
(About 53,000)

2012 3rd Quarter
structure and numbering of jvn.
Numbering and Vulnerability Reporting

1. Report
2. Verification
3. Forward report
4. Identification of affected vendors from DB
5. Notification of vulnerability related information - Test suite and validation process
6. Coordination of announcement date
7. Investigation and make countermeasures
8. Submission of security information
9. Announcement

International Framework
Notification

Coordination Body
JPCERT/CC
CVE-2012-1234

Japan Vulnerability Notes
JVN#1234567

IPA#12345678
JVNDB-yyyy-123456

End User
Cooperate Users
System Integrators
ISP
Distributors

IPA
Information-technology Promotion Agency, Japan
- Structure and numbering of JVN
- JVN Security Content Automation Framework
- MyJVN project
JVN Security Content Automation Framework (aka. MyJVN framework) has adopted SCAP.
related activities (phase 1).
JVN Security Content Automation Framework

▲ Jun 2002: JVN working group formed
▲ Feb 2003: Trial site (jvn.doi.ics.keio.ac.jp) to the public
▲ Jul 2003: JVNRSS stared

▲ Jul 7, 2004: Information security early warning partnership

▲ Jan 2006: Evaluating CVSS V1.0 for adoption
▲ Sep 2006: CVSS V1.0 Calculator [CN][NL][EN][DE][JA][KO][PT][ES]

▲ Apr 2007: **JVN iPedia (aka. Vuln. archiving DB)**
  http://jvndb.jvn.jp/ (Adopted CVE and CVSS)
▲ Aug 2007: Adopted CVSS V2.0 in JVN iPedia

▲ May 2008: English Versions of JVN and JVN iPedia
▲ Sep 2008: JVN iPedia extension (Adopted CWE)
▲ Sep 2008: JVN iPedia extension (CVE Declaration)
related activities (phase 2).
JVN Security Content Automation Framework

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008</td>
<td>Sep 2008: MyJVN project started</td>
</tr>
<tr>
<td></td>
<td>Oct 2008: JVN iPedia extension (Adopted CPE)</td>
</tr>
<tr>
<td></td>
<td>Oct 2008: MyJVN Filtered vulnerability information tool (Adopted CPE)</td>
</tr>
<tr>
<td></td>
<td>Nov 2009: MyJVN Version Checker (VC) (Adopted CPE and OVAL)</td>
</tr>
<tr>
<td></td>
<td>Dec 2009: MyJVN Security Configuration Checker (SCC) (Adopted OVAL, CCE and XCCDF)</td>
</tr>
<tr>
<td>2010</td>
<td>Jan 2010: JVN, JVN iPedia and MyJVN (CVE-Compatible)</td>
</tr>
<tr>
<td></td>
<td>Jan 2010: CVSS V2.0 Calculator [AR][EN][FR][DE][JA][KO][ES]</td>
</tr>
<tr>
<td>2012</td>
<td>Feb 2010: MyJVN API (Filtered information service API)</td>
</tr>
<tr>
<td></td>
<td>Jun 2010: MyJVN - VRDA collaboration</td>
</tr>
<tr>
<td>2013</td>
<td>Mar 2011: MyJVN VC and MyJVN SCC (OVAL Adopter)</td>
</tr>
<tr>
<td>2016</td>
<td>Aug 2012: MyJVN API (SCAP collaboration service API)</td>
</tr>
</tbody>
</table>
• Structure and numbering of JVN
• JVN Security Content Automation Framework
• MyJVN project
myjvn project. = SCAP collaboration activities

- **Operational View**
  - CWE-Compatible (Oct 3, 2008)
  - CVE-Compatible (JVN, JVN iPedia and MyJVN) (Jan 5, 2010)
  - CAN (CVE Numbering Authority) (Jun 24, 2010)
  - OVAL Adopter (MyJVN VC and MyJVN SCC) (Mar 15, 2011)
myjvn project.
= SCAP collaboration activities

- Operational View
  - CWE- Compatible (Oct 3, 2008)
  - CVE- Compatible (JVN, JVN iPedia and MyJVN) (Jan 5, 2010)
  - CAN (CVE Numbering Authority) (Jun 24, 2010)
  - OVAL Adopter (MyJVN VC and MyJVN SCC) (Mar 15, 2011)
myjvn project.
= SCAP collaboration activities

- Technical View
  - JVN
  - JVN iPedia
  - CVSS Calculator
  - MyJVN API
  - MyJVN Filtered Vulnerability Countermeasure Information Tool
  - MyJVN Version Checker (VC)
  - MyJVN Security Configuration Checker (SCC)
  - Collaboration possibilities of CPE
July 2004, "Japan Vulnerability Notes (JVN) (aka. Vulnerability handling coordination DB)" started the portal site of security information of domestic product vendors under the vulnerability information handling framework in Japan.

- Vulnerability handling coordination DB assists system administrators and software and other products developers enhance security for their products and customers.
  - **Vulnerability Notes (VN)**
  - **Status Tracking Notes (TRnotes)** (currently in trial operation)
VN includes a list of JP product vendors who may be affected by the vulnerability.

There are five categories as Status.
- Unknown
- Vulnerable (Completed investigation)
- Vulnerable (Under investigation)
- Not Vulnerable (Completed investigation)
- Not Vulnerable (Under investigation)

JVN#12345678
Cross-site scripting vulnerability in Apache HTTP Server "mod_imap" and "mod_imagemap"

Overview
mod_map and imagemap modules in Apache servers are vulnerable to cross-site scripting.

Vendor Status

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Status</th>
<th>Last Update</th>
<th>Vendor Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hitachi</td>
<td>Vulnerable</td>
<td>2007/12/13</td>
<td></td>
</tr>
<tr>
<td>NEC Corporation</td>
<td>Not Vulnerable, investigating</td>
<td>2007/12/13</td>
<td></td>
</tr>
<tr>
<td>Century Systems Co., Ltd</td>
<td>Not Vulnerable, investigating</td>
<td>2007/12/13</td>
<td></td>
</tr>
<tr>
<td>FUJITSU LIMITED</td>
<td>Vulnerable, investigating</td>
<td>2008/01/17</td>
<td></td>
</tr>
<tr>
<td>Canon Inc.</td>
<td>Not Vulnerable</td>
<td>2008/03/20</td>
<td></td>
</tr>
</tbody>
</table>

Reference
The Apache Software Foundation, Apache 2.2 Security Vulnerabilities CVE-2007-5000
# jvn - vulnerability notes (vn).

http://jvn.jp/en/

## Recent Vulnerability Notes

<table>
<thead>
<tr>
<th>JVN#</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>01635457</td>
<td>e107 vulnerable to cross-site scripting</td>
<td>March 14, 2011</td>
</tr>
<tr>
<td>81294135</td>
<td>IBM Tivoli vulnerable to denial-of-service (DoS)</td>
<td>March 10, 2011</td>
</tr>
<tr>
<td>73162541</td>
<td>OTRS vulnerable to OS command</td>
<td>2011 12:00</td>
</tr>
<tr>
<td>97334690</td>
<td>IBM Lotus vulnerable to denial-of-service (DoS)</td>
<td>March 04, 2011</td>
</tr>
<tr>
<td>26301278</td>
<td>IBM WebSphere Application Server vulnerable to denial-of-service (DoS)</td>
<td>March 14, 2011</td>
</tr>
</tbody>
</table>

## JVN#88991166

### SEIL Series routers vulnerable to buffer overflow

#### Overview

SEIL Series routers contain a buffer overflow vulnerability.

#### Products Affected

- SEILA6 firmware 1.00 to 1.61
- SEIL/B1 firmware 1.00 to 3.11
- SEIL/X1 firmware 1.00 to 3.11
- SEIL/X2 firmware 1.00 to 3.11
jvn - vulnerability notes (vn).
http://jvn.jp/en/
The purpose of TRnotes is in sharing the events of time series. The event information is based on public information.

---

Event Information includes followings.
- Discovered date of vulnerability
- Published date of any advisories
- Released date of exploit code
- Discovered date of worm
- Published alerts from governments. etc.

---

Published: 2008-08-24T09:40:00  Last Updated: 2008-08-31T04:54:00

TRTA08-190B
Multiple DNS implementations vulnerable to cache poisoning

Overview
Deficiencies in the DNS protocol and common DNS implementations facilitate DNS cache poisoning attacks. Effective attack techniques against these vulnerabilities have been demonstrated.

Event Information

<table>
<thead>
<tr>
<th>Date (UTC)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008-08-24</td>
<td>ICANN</td>
</tr>
<tr>
<td></td>
<td>Domain Name Security Paper Released</td>
</tr>
<tr>
<td></td>
<td>ICANN’s strategic and operating plans call for ICANN to be operationally ready to deploy DNSSEC at the root level and work with relevant stakeholders to determine how this standard will be implemented.</td>
</tr>
<tr>
<td></td>
<td>Office of Management and Budget</td>
</tr>
<tr>
<td></td>
<td>M-08-23: Securing the Federal Government’s Domain Name System Infrastructure (Subn Draft Agency Plans Due by September 5, 2008)</td>
</tr>
<tr>
<td></td>
<td>The memorandum describes existing and new policies for deploying Domain Name System Infrastructure security.</td>
</tr>
</tbody>
</table>

---

Information-technology Promotion Agency, Japan
JVN iPedia

- JVN iPedia (aka. Vulnerability archiving DB) focuses on regional vulnerabilities (which depends on IT market) in Japan.
- Vulnerability archiving DB stores summary and countermeasure information on vulnerabilities in Japanese software and other products posted on JVN.
The "Ichitaro" series word processing software contains a buffer overflow vulnerability.

This vulnerability is different from JVN#29211062, JVN#32981509 and JVN#50495547.

The "Ichitaro" series word processing software, from JustSystems Corporation, contains an issue in the reading of Rich Text Files resulting in a
1. JVN: JVN#33846134
2. IPA SECURITY ALERTS: Security Alert for Security Vulnerability in the Ichitaro Series
5. Secunia Advisory: SA34611
6. SecurityFocus: 34403
7. ISS X-Force Database: 49739
8. VUPEN Security: VUPEN/ADV-2009-0957
9. OPEN SOURCE VULNERABILITY DATABASE (OSVDB): 53349
10. Common Weakness Enumeration (CWE): Failure to Constrain Operations within the Bounds of a Memory Buffer (CWE-119) [IPA Evaluation]

This vulnerability is different from JVN#29211062, JVN#32981509 and JVN#50495547.

The "Ichitaro" series word processing software, from JustSystems Corporation, contains an issue in the reading of Rich Text Files resulting in a...
jvn ipedia.
http://jvndb.jvn.jp/en/

XML format = RSS1.0+mod_sec

Information-technology Promotion Agency, Japan
CVSS V2.0 Calculator

- Graphical user interface: 5 Themes
- Multi languages supported: 7 Languages (Oct 2010)

http://jvndb.jvn.jp/en/
CVSS V2.0 Calculator loads parameter XML file such as Arabic, English and etc.

JVN thanks the following for working with us:
Arabic: Supported by Helmi Rais (http://www.first.org/)
French: Supported by Helmi Rais (http://www.first.org/)
German: Supported by Farim Nawabi and Akira Yamada
Korean: Supported by KISA (http://www.kisa.or.kr)
Spanish: Supported by Francisco Jesus Monserrat Colla (http://www.first.org/)

Information-technology Promotion Agency, Japan
MyJVN API

- A software interface to access and utilize vulnerability countermeasure information stored in JVN iPedia, with testing support tools.

- To enable application developers to use data through open interface, JVN iPedia has adopted SCAP, a set of standards for describing vulnerability countermeasure information.
A custom applications can access the data in JVN iPedia and various vulnerability management services can now efficiently utilize vulnerability countermeasure information.

Filtered information service API
- JPCERT/CC VRDA collaboration
- MyJVN Filtered Vulnerability Countermeasure Information Tool

SCAP collaboration service API
- MyJVN Version Checker
- MyJVN Security Configuration Checker

myjvn api.
Filtered information service API

- **Get Vendor List**
  The vendor list that is filtered by the CPE is acquired in XML format.

- **Get Product List**
  The product list that is filtered by the CPE is acquired in XML format.

- **Get Vulnerability Overview List**
  The vulnerability overview list that is filtered by the CPE is acquired in JVNRSS (RSS + mod_sec) format.

- **Get Vulnerability Detail Information**
  The vulnerability detail information is acquired in VULDEF format.
Filtered information service API

- **Get Vendor List**
  
  http://jvndb.jvn.jp/myjvn?method=getVendorList&cpeName=cpe:/*:j*&lang=en

- **Get Product List**
  
  http://jvndb.jvn.jp/myjvn?method=getProductList&cpeName=cpe:/*:sony:*&lang=en

- **Get Vulnerability Overview List**
  
  http://jvndb.jvn.jp/myjvn?method=getVulnOverviewList&cpeName=cpe:/*:fujitsu:*&rangeDatePublic=n&rangeDatePublished=n&rangeDateFirstPublished=n&lang=en

- **Get Vulnerability Detail Information**
  
filtered information service api.

- XML formats
  - Using JVNRSS, an XML format to describe the overview, is an essential point in the security information exchange.

Overview Format

JVNRS 2.0 = RSS1.0+mod_sec

MyJVN API
getVulnOverviewList

Overview Format

JVNRS 2.0
<sec:identifier>Unique identifier assigned by vendor</sec:identifier>
<sec:references>Best reference to a related security information</sec:references>
<sec:cvss score="Overall score"
    severity="Severity level (High - Medium - Low)"
    vector="Value of each vector in CVSS"
    version="CVSS version"/>
<sec:cpe-item name="CPE Name">
    <sec:vname>Vendor Name</sec:vname>
    <sec:title>Product Name</sec:title>
</sec:cpe-item>

MyJVN API
getVulnDetailInfo

JVNRSS: Japan Vulnerability Notes RSS
mod_sec: Qualified Security Advisory Reference
VULDEF: The VULnerability Data publication and Exchange Format data model
filtered information service api.
myjvn api.

- SCAP collaboration service API
  - Get list of OVAL definition
    The OVAL definition list is acquired in XML format.

  - Get list of XCCDF configuration
    The XCCDF configuration data list is acquired in XML format.

  - Get Data of OVAL definition
    The OVAL definition file is acquired in enveloped OVAL format.

  - Get Data of XCCDF configuration
    The XCCDF configuration data is acquired in enveloped XCCDF format.
• SCAP collaboration service API
  - Get list of OVAL definition
  - Get list of XCCDF configuration
    http://jvndb.jvn.jp/myjvn?method=getXccdfList
  - Get Data of OVAL definition
  - Get Data of XCCDF configuration
myJVN tools.

Filtered security information for your system

Improvement of the keeping environment on your PC

Filtered version checker

Information technology Promotion Agency, Japan
To efficiently gather only relevant information from the vast quantity of data stored in JVN iPedia, the vulnerability countermeasure information database.

myjvn filtered security information tool:

Filtering Result Window

Detailed Information Window

Overview
Apache Tomcat from the Apache Software Foundation contains a vulnerability that could allow a remote attacker to gain control over a user’s web browser. Apache Tomcat from the Apache Software Foundation is a web container for Java Servlets and JavaServer Pages. The developers report that this issue exists because of an incomplete...
myjvn version checker.
http://jvndb.jvn.jp/apis/myjvn/vccheck.html

- Improvement of the keeping up-to-date environment
  - Splitting the keeping up-to-date steps into two phase.
    - Step 1: Check phase ... MyJVN - Version Checker
      Is your PC keeping the latest version?
    - Step 2: Remedy phase ... Our Next issue
      Let's update the applications and the plug-ins on your PC.

```
<table>
<thead>
<tr>
<th>Product Name (ascending)</th>
<th>Results</th>
<th>Details (ascending)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Flash Player (ActiveX)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adobe Flash Player (Plug-in)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adobe Reader</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JRE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thunderbird</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mozilla Thunderbird</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QuickTime</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
MyJVN Version Checker supports multi platforms and multi products.

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP, Vista, 7, 8</td>
<td>Adobe Flash Player</td>
</tr>
<tr>
<td>Windows 2003, 2008</td>
<td>Adobe Reader</td>
</tr>
<tr>
<td>CentOS 5, Red Hat Enterprise Linux 5</td>
<td>Adobe Shockwave Player</td>
</tr>
<tr>
<td></td>
<td>JRE</td>
</tr>
<tr>
<td></td>
<td>Lhaplus</td>
</tr>
<tr>
<td></td>
<td>Mozilla Firefox</td>
</tr>
<tr>
<td></td>
<td>Mozilla Thunderbird</td>
</tr>
<tr>
<td></td>
<td>QuickTime</td>
</tr>
<tr>
<td></td>
<td>Lunascape</td>
</tr>
<tr>
<td></td>
<td>Becky! Internet Mail</td>
</tr>
<tr>
<td></td>
<td>OpenOffice.org</td>
</tr>
<tr>
<td></td>
<td>VMware Player</td>
</tr>
</tbody>
</table>
Improvement of the keeping the secure configuration on your PC

- Splitting the steps into Check and Remedy phase.

<table>
<thead>
<tr>
<th>Check Item</th>
<th>Recommended Value</th>
<th>PC Setting Value</th>
<th>Check Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Password Length</td>
<td>12 characters</td>
<td>CCE-2981-9</td>
<td></td>
</tr>
<tr>
<td>Maximum Password Age</td>
<td>60 days</td>
<td>CCE-2920-7</td>
<td></td>
</tr>
<tr>
<td>Password History</td>
<td>24 times</td>
<td>CCE-2994-2</td>
<td></td>
</tr>
<tr>
<td>Minimum Password Age</td>
<td>1 day</td>
<td>CCE-2439-8</td>
<td></td>
</tr>
<tr>
<td>Account Lockout Threshold</td>
<td>5 times</td>
<td>CCE-2986-8</td>
<td></td>
</tr>
<tr>
<td>Password Reset Duration</td>
<td>15 minutes</td>
<td>CCE-2466-1</td>
<td></td>
</tr>
<tr>
<td>Account Lockout Duration</td>
<td>15 minutes</td>
<td>CCE-2928-0</td>
<td></td>
</tr>
<tr>
<td>Password Protect Screen Saver</td>
<td>Effective</td>
<td>CCE-4500-5</td>
<td></td>
</tr>
<tr>
<td>Autorun Disable</td>
<td>Effective</td>
<td>CCE-2154-3</td>
<td></td>
</tr>
</tbody>
</table>

Information-technology Promotion Agency, Japan
MyJVN Security Configuration Checker supports two platforms, the CCEs for password and lockout policies.

Platforms
- Windows XP, Vista, 7, 8
- CentOS 5, Red Hat Enterprise Linux 5

CCEs for password and lockout policies
- CCE-2981-9: The "minimum password length" policy
- CCE-2920-7: The "maximum password age" policy
- CCE-2994-2: The "enforce password history" policy
- CCE-2439-8: The "minimum password age" policy
- CCE-2986-8: The "account lockout threshold" policy
- CCE-2466-1: The "reset account lockout counter after" policy
- CCE-2928-0: The "account lockout duration" policy
- CCE-2980-1: The "Screen Saver Timeout" setting should be configured correctly for the current user.
- CCE-4500-5: The "Password protect the screen saver" setting should be configured correctly for the current user.
MYJI.IN is the framework of machine readable environment with the common enumeration based as a security information sharing and exchanging.

References

- **JVN (Vulnerability Handling Coordination DB)**
  http://jvn.jp/en/

- **JVN iPedia (Vulnerability Archiving DB)**
  http://jvndb.jvn.jp/en/

- **MyJVN**

- **JVN RSS (JP Vendor Status Notes RSS) Feasibility Study Site**
  http://jvnrsseise.chuo-u.ac.jp/jtg/

- **Information Security Early Warning Partnership**
  http://www.ipa.go.jp/security/english/quarterlyrep_vuln.html#Partnership
References

- **JVN RSS (Japan Vulnerability Notes RSS)**
  namespace="http://purl.org/rss/1.0/"
  schemaLocation="http://jvndb.jvn.jp/schema/jvnrss_2.0.xsd"

- **Qualified Security Advisory Reference (mod_sec)**
  namespace="http://jvn.jp/rss/mod_sec/"
  schemaLocation="http://jvndb.jvn.jp/schema/mod_sec_2.0.xsd"

- **VULDEF**
  The VULnerability Data publication and Exchange Format data model
  namespace="http://jvn.jp/vuldef/"
  schemaLocation="http://jvndb.jvn.jp/schema/vuldef_2.0.xsd"
Thank you

Structure and numbering of JVN, and Security content automation framework

November 14, 2012

Masato Terada

Security Engineering Laboratory, IT Security Center (ISEC)
IPA (Information-technology Promotion Agency, Japan)