Proposal of RSS Extension for Security Information Exchange

18th Annual FIRST Conference
2006/06/30

Masato Terada
m-terada@ipa.go.jp
http://jvn.jp/
Opening

We propose JVNRSS (JP Vendor Status Notes RSS) as a security information sharing and exchanging specification. JVNRSS is based on RSS 1.0 and uses the "<dc:relation>" field defined in the Dublin Core as a Relational ID to correlate security information issued by various sources. JVNRSS uses the reference URL specified in a security alert, for example, an URL of the Common Vulnerability Exposure, CERT Advisory, CERT Vulnerability Note and CIAC Bulletin.

In this presentation, firstly we'll explain the specification and applications of JVNRSS. Secondly, we'll introduce the result of our feasibility study on JVNRSS and lastly we'll propose the RSS Extension for security information sharing.
Contents

1. Vulnerability Information Handling Framework in Japan
2. JVN: JP Vendor Status Notes
Vulnerability Information Handling Framework in Japan
1. Vulnerability Information Handling Framework in Japan

Under “the Guideline for Handling Vulnerability-related Information”
Announced on July 7, 2004, into Effect on July 8, 2004

Government-private sector cooperation to promote a smooth information flow concerning vulnerabilities and countermeasures of software products/web site applications. The first vulnerability information handling mechanism that is based on the official rules.

**Expected Effects**

1. Promote proactive vulnerability response by vendors/web site operators
2. Curb neglect and improper publication of vulnerability information
3. Prevent leak of sensitive information and disruption of critical systems
1. Handling Framework for Vulnerability of Software Product

- The Software Vulnerabilities Handling Framework defines the operational process for vulnerability information handling from a vulnerability’s discovery to its release to the public.
  - Report a vulnerability to IPA
  - Coordinate the vulnerability information handling between JPCERT/CC and JP product vendors
  - Investigate and eliminate vulnerabilities in the products of each JP vendor
  - Announce security information on JVN

- JPCERT/CC collaborates with CERT/CC and NISCC on vulnerability information handling in the International framework.
1. Handling Framework for Vulnerability of Software product

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 countermeasure
8. Submission of security information
9. Announcement

Coordination Body (JPCERT/CC)

Receipt Body (IPA)

JP Vendor Status Notes VN-JP

End User
Cooperate Users
System Integrators
ISP
Distributors

International Framework Notification
1.

Vulnerabilities reported Statistics 2004-2006

Vulnerabilities

- Vuln. of Software products
- Vuln. of Web sites

<table>
<thead>
<tr>
<th>Year/Quarter</th>
<th>Vuln. of Software Products</th>
<th>Vuln. of Web Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004/3Q</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>2004/4Q</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>2005/1Q</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>2005/2Q</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>2005/3Q</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>2005/4Q</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>2006/1Q</td>
<td>34</td>
<td></td>
</tr>
</tbody>
</table>

http://www.ipa.go.jp/security/index-e.html
JVN: JP Vendor Status Notes

http://jvn.jp/
2. JVN History

- JVN project started in 2003 to make a portal site of security information of domestic product vendors in Japan.

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>2002/06 JVN Project Started</td>
</tr>
</tbody>
</table>
| 2003 | - 2003/02 jvn.doi.ics.keio.ac.jp Opened to public.  
- 2003/07 JVN RSS channel service Opened to public.  
- 2004/01 TRnotes service Opened to public.  |
| 2004 | 2004/07 jvn.jp Opened to public. |
| 2005 | |

1st Step (Trial Site)
JVN: JPCERT/CC Vendor Status Notes
February 3, 2003
URL http://jvn.doi.ics.keio.ac.jp
Email jvn@doi.ics.keio.ac.jp

2nd Step
JVN: JP Vendor Status Notes
July 8, 2004
URL http://jvn.jp/
Email jvn@jvn.jp
2. Overview of JVN

- July 2004, “JP Vendor Status Notes (JVN)” was launched as a portal site to offer security information on domestic product vendors under the vulnerability information handling framework in Japan.
  - Provide the Vendor Status Notes (VN) and the status Tracking Notes (TRnotes).
  - **“Vendor Status Notes (VN)”** VN is a service providing information on how to fix vulnerabilities. It is similar to the “CERT Vulnerability Notes” and follows up the IPA/JPCERT Vulnerability reports, US-CERT Alerts, US-CERT Vulnerability Notes and NISCC Advisories.
  - **“Status Tracking Notes (TRnotes)”** is a service providing information on the incidents, specifically what worms do, when the exploit codes were released and what the countermeasures are.
“JP Vendor Status Notes (JVN)” has four information categories.

- VN-JP
- VN-CERT/CC
- VN-NISCC
- TRnotes

http://www.ipa.go.jp/
http://www.jpcert.or.jp/
2. VN-CERT/CC

Notified via CERT/CC

2004-07-08: Public Opened
2004-07-20: Workshop of Vulnerability Information Handling

VN-NISCC

Notified via NISCC

TRnotes

2004-07-08: Public Opened
2004-07-20: Workshop of Vulnerability Information Handling

2004-07-08: Multiple SSL-VPN products fail to set the "Secure" attribute of a cookie
2004-07-20: desknet's vulnerable to script execution via certain HTML mail
2004-07-20: Virus Baster Cooperate Edition vulnerable to information leak

Multiple vulnerabilities in Mozilla products
Microsoft Windows JPEG component buffer overflow
Vulnerabilities in MIT Kerberos 5
Vulnerability Issues with Business Objects WebIntelligence Product
Vulnerability Issues with the Apache Web Server
Vulnerability Issues in MIME
W32/Novarg.A Virus
Multiple vulnerabilities in Mozilla products
Vendor Status Notes (VN)

- "Vendor Status Notes (VN)" includes a list of JP product vendors who may have been affected by the reported vulnerabilities.
  - VN has three information categories such as VN-JP, VN-CERT/CC and VN-NISCC.
  - Each web page consists of the overview of the problem, its impact, vendor information and related information.

<table>
<thead>
<tr>
<th>JVN#12345678</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
</tr>
<tr>
<td>Overview</td>
</tr>
<tr>
<td>Impact</td>
</tr>
<tr>
<td><strong>Vendor Information</strong></td>
</tr>
<tr>
<td>Reference</td>
</tr>
<tr>
<td>Revisions</td>
</tr>
</tbody>
</table>

Vendor Information includes Vendor Name, Status and Last Update. There are five categories as Status.

- **Unknown**
- **Vulnerable**
  - Vulnerable (Completed investigation)
  - Vulnerable (Under investigation)
- **Not Vulnerable**
  - Not Vulnerable (Completed investigation)
  - Not Vulnerable (Under investigation)
Multiple Vulnerabilities in libpng

Overview

Several vulnerabilities exist in the libpng library, the most serious of which could allow a remote attacker to execute arbitrary code on an affected system.

Impact

A remote attacker could cause an application to crash or potentially execute arbitrary code by convincing a victim user to visit a malicious web site or view an email message containing a malformed image.

Vendor Information

Product Vendor List

<table>
<thead>
<tr>
<th>Vendor Name</th>
<th>Status</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fujitsu</td>
<td>Not Vulnerable (Completed investigation)</td>
<td>2004/08/26</td>
</tr>
<tr>
<td>MIRACLE Linux</td>
<td>Vulnerable (Completed investigation)</td>
<td>2004/08/24</td>
</tr>
<tr>
<td>Turbo Linux</td>
<td>Vulnerable (Completed investigation)</td>
<td>2004/08/23</td>
</tr>
<tr>
<td>TechMatrix</td>
<td>Not Vulnerable (Completed investigation)</td>
<td>2004/08/17</td>
</tr>
</tbody>
</table>
“Status Tracking Notes (TRnotes)” includes a list of event/time information on incidents concerning vulnerabilities.

- Each web page consists of the overview, timeline concerning a vulnerability and related information.
- The purpose of TRnotes is in sharing the timeline of the incident, which includes worm activities, the date exploit codes were released and the countermeasure against security incidents. The information is based on public information.

Event Information includes followings.

- Date the vulnerability was discovered
- Date any advisories are released
- Date exploit codes are published
- Date worms are produced
- Published alerts from governments.
- Additional resources, such as a government agency etc.
### Microsoft Windows JPEG component buffer overflow

<table>
<thead>
<tr>
<th>Time (JST)</th>
<th>Event Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004-09-17 04:58</td>
<td>ISSK <a href="#">TA04-250A</a></td>
</tr>
<tr>
<td>2004-09-20 03:38</td>
<td>Full-Disclosure &quot;Microsoft Windows MS04-026 JPEG Overflow Shellecode Exploit&quot;</td>
</tr>
<tr>
<td>2004-09-23 15:22</td>
<td>Bugtraq <a href="#">NEW GDI+ JPEG Remote Exploit</a></td>
</tr>
<tr>
<td>2004-09-23 23:55</td>
<td>ISSK <a href="#">AlertCon</a></td>
</tr>
<tr>
<td>2004-09-24 13:49</td>
<td>ISSKK announces an alert &quot;Microsoft GDI+ JPEG Processing Exploitation&quot;.</td>
</tr>
</tbody>
</table>
Proposal of RSS Extension for Security Information Exchange
How we can provide a more efficient security information distribution service for the security administrators that helps them reduce their workload related to collecting and grouping various information and take care of security incidents.

Distribution designed to encourage reusing of information

More efficient aggregation of information from product vendors
Keywords for the solution
- Semantic Web
- RSS (RDF Site Summary)

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

<table>
<thead>
<tr>
<th>Format for the overview</th>
<th>Format for the details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>JVNRSS</strong></td>
<td><strong>VULDEF and others</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Title</th>
<th>Overview</th>
<th>Affected System</th>
<th>Impact</th>
<th>Solution</th>
<th>Exploit</th>
<th>Reference</th>
</tr>
</thead>
</table>

Copyright © JVN. 2006. All rights reserved.
JVN RSS Specification

- **JVN RSS**
  - Summary format for security information exchange.
  - Based on RSS 1.0 and use the field `<dc:relation>` of Dublin Core as index of grouping security information.

```xml
<item rdf:about="URL of security information">
  <title>Title</title>
  <link>URL of security information</link>
  <description>Outline of security information</description>
  <dc:publisher>Product vendor name</dc:publisher>
  <dc:creator>Contact point information</dc:creator>
  <dc:identifier>Security information ID</dc:identifier>
  <dc:relation>Relational ID (1) {CVE|CERT-CA|CERT-VU|etc.}</dc:relation>
  <dc:relation>Relational ID (2) {CVE|CERT-CA|CERT-VU|etc.}</dc:relation>
  <dc:date>Date last updated</dc:date>
  <dcterms:issued>Date first published</dcterms:issued>
  <dcterms:modified>Date last updated</dcterms:modified>
</item>
```
3. JVNRS Example

- **ID**: JVNVU#834865
- **Title**: Sendmail contains a race condition
  - **Reference**: http://www.us-cert.gov/cas/techalerts/TA06-081A.html
  - **Reference**: http://www.kb.cert.org/vuls/id/834865
  - **Reference**: http://cve.mitre.org/cgi-bin/cvename.cgi?name=2006-0058

```xml
<Item rdf:about="http://jvn.jp/cert/JVNVU%23834865">
  <Title>Sendmail contains a race condition</Title>
  <Link>http://jvn.jp/cert/JVNVU%23834865</Link>
  <Description>A race condition in Sendmail may allow a remote attacker …</Description>
  <DC:publisher>JVNRS-DEV project</DC:publisher>
  <DC:creator>jvn@jvn.jp</DC:creator>
  <DC:identifier>JVNVU#834865</DC:identifier>
  <DC:date>2006-04-03T10:30+09:00</DC:date>
  <DC:issued>2006-03-23T04:00+09:00</DC:issued>
  <DC:modified>2006-04-03T10:30+09:00</DC:modified>
</Item>
```
3. JVNRS Application: Visualized JVNRS

- Offer the summary of JVN articles through other websites.
3. **JVNRSS Application: Visualized TRnotes**

- Arrange all events by time.

```xml
  <title>[Full-disclosure] (MS05-039) Microsoft Windows Plug-and-Play Service Remote Overflow (Universal Exploit + no crash shellcode)</title>
  <dc:date>2005-08-12T23:37+09:00</dc:date>
</item>
```
3. JVNRS Application: Security information gathering system

- Reduce workload in collecting and grouping security information.

(3) Convert XML to HTML

(2) Grouping of the security information.

(1) Gathering of the security information.
3. JVNRRSS Application: Proposal grouping (correlation) mechanism

- The grouping mechanism using Relational ID without mapping DB.

(3) Convert XML to HTML

- JVN Sites
  - CA-2003-04
    - Vendor A
    - Vendor B
    - News X

- Convert module
  - Grouping module
    - Mapping DB
    - CERT-CA
    - CVE etc
  - Gathering module
    - Archive DB

(2) Grouping of the security information.

(1) Gathering of the security information

Vendor A Site


News X Site


match

CA-2003-04

CA-2003-04

YES

CA-2003-04

YES

CA-2003-04

YES
3. JVN RSS Application: Proposal grouping (correlation) mechanism

- The grouping mechanism using Relational ID with mapping DB.

(3) Convert XML to HTML

(2) Grouping of the security information.

Mapping DB entry

- CVE-2004-0230
- TA04-111A
- XF15886
- VU#415294
- BID10183

- CA-2003-20
- CIAC Bulletin N-133
- JPCERT-AT-2003-0005
- JPCERT-AT-2003-0006

Gathering module

Convert module
3. JVNRS: Proposal grouping (correlation) mechanism

- The grouping mechanism using Relational ID with mapping DB.

(3) Convert XML to HTML

<table>
<thead>
<tr>
<th>JVN Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA-2003-04</td>
</tr>
<tr>
<td>- Vendor A</td>
</tr>
<tr>
<td>- Vendor B</td>
</tr>
<tr>
<td>- News X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Convert module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grouping module</td>
</tr>
<tr>
<td>Gathering module</td>
</tr>
</tbody>
</table>

| Mapping DB |
| CERT-CA|
| CVE etc |

| Archive DB |

(2) Grouping of the security information.

(1) Gathering of the security information

Vendor A Site

- <item rdf:about="http://A.JP/alert-sql.html">
  <title>SQL Slammer worm information</title>
  <link>http://A.JP/alert-sql.html</link>
  <dc:relation>415294</dc:relation>
</item>

News X Site

  <title>SQL Slammer worm information</title>
</item>

- VU#415294
- YES
- match

Copyright © JVN. 2006. All rights reserved.
3. JVN RSS practical activity

- **CVE+**  
  http://jvnrs.isb.chuo-u.ac.jp/jtg/cve+/  
  CVE+ is to make a relationship map between CVE and Japanese security information.

- **TRnotes**  
  http://jvnrs.isb.chuo-u.ac.jp/jtg/trn/  
  TRnotes provides HTML based information, JVN RSS format and Visualized TRnotes.

- **XSL_swf**  
  http://jvnrs.isb.chuo-u.ac.jp/jtg/xswf/  
  XSL_swf is FLASH tool for visualized JVN RSS and uses a part of XSL as a mechanism to describe how the document should be displayed.

- **RSS_dir**  
  http://jvnrs.isb.chuo-u.ac.jp/jtg/rssd/  
  RSS_dir is concept of RSS directory for RSS channel. RSS directory describes a RSS channel tree with RSS format.

- **SIG_rdf**  
  http://jvnrs.isb.chuo-u.ac.jp/jtg/xsig/
Prototype system

**Modules:** gathering, grouping and convert

**Viewer**
- TouchGraph Link Browser
- MAP Viewer
- LIST Viewer
- Web Browser

**Data Format**
- TouchGraph XML
- JVNRS <sec:item>
- HTML

**Mapping DB data source**
- CVE.mitre.org
- NVD.nist.gov
- cve.xml
- nvd.xml

**Archive DB data source**
- site.A
- site.B
- jvnrss.rdf
- jvnrss.rdf

**Convert module**
- Grouping module
- Gathering module
- Mapping DB
- Archive DB
3. JVNRRSS practical activity

- **Viewer:** TouchGraph Link Browser (Java Applet)
- **Data Format:** TouchGraph XML format

```xml
<NODESET>
  <NODE nodeID="CVE_2004-0230">
    <NODE_LABEL label="CVE CVE-2004-0230"/>
  </NODE>
  <NODE nodeID="CERT_TA04-111A">
    <NODE_LABEL label="US-CERT TA04-111A"/>
  </NODE>
  <EDGE fromID="CVE_2004-0230" toID="CERT_TA04-111A"/>
</NODESET>
```
3. JVNRSY practical activity

- **Viewer**: Map Viewer (SWF)
  - **Data Format**: TouchGraph XML format

```xml
<EDGESET>
<EDGE fromID="CVE_2004-0230" toID="CERT_TA04-111A" />
</EDGESET>

<NODESET>
<NODE nodeID="CVE_2004-0230">
<NODE_LABEL label="CVE CVE-2004-0230" />
</NODE>
<NODE nodeID="CERT_TA04-111A">
<NODE_LABEL label="US-CERT TA04-111A" />
</NODE>
</NODESET>
```
3. **JVNRSS practical activity**

- **Viewer:** LIST Viewer (SWF)
  - **Data Format:** JVNRS + <sec:item> format

```xml
<item rdf:about="http://www.us-cert.gov/cas/...">
  <title>TA04-111A</title>
  <sec:item>
    <item rdf:about="http://jvn.jp/cert/JVNTA04-111A">
      <title>Potential Reliability Issue in TCP</title>
    </item>
    <item rdf:about="http://www.hitachi.co.jp/...">
      <title>GR2000/GR4000/GS4000/GS3000 ...</title>
    </item>
  </sec:item>
</item>
```
XSL_swf is a FLASH tool for the visualized JVNRSS

- XSL_swf refers to an XSL file to describe how a document should be displayed.
RSS_dir is a concept of the RSS directory for the RSS channel. RSS directory describes a RSS channel tree using the RSS format.

- Check the feed for changes and react to the changes in an appropriate way
3. JVN RSS practical activity

- Use RSS_dir to selectively display the information collected/updated in the last 7 days

**Step 1:** Read top layer RDF

- **jp_root.rdf**

**Step 2:** Read 2nd layer RDFs

- **vendorA.rdf**
- **vendorB.rdf**

*Updated in the last 7 days*
3. Proposal RSS Extension

- JVN RSS is based RSS 1.0 and a proprietary format in Japan.
- Exchange security information in worldwide.
- The ability to use RSS holds the key to successfully implement a scheme for distributing security related information.
- Qualified Security Advisory Reference (mod_sec)
  RSS Extension definition of the tags for RSS 1.0, RSS 2.0 and Atom
sec:references is an element for a best reference (CVE, CERT Advisory, CERT Vulnerability Note, US-CERT Technical Alert etc.) to related security information.

Syntax

```
<sec:references sec:source="%name" sec:id="%id"> %ResourceReference </sec:references>
```

- **%name**
  An attribute is abbreviation name, which provides the best reference, such as CVE, JPCERT, CERT, CIAC, BID, CERT-VN, MS, OSVDB, XF etc.

- **%id**
  An attribute is the unique identifier assigned by sec:source, such as VU#105259, MS01-044, CVE-2001-0525, CA-2001-14, TA05-111A etc.

- **%ResourceReference**
  An entity value is a URI reference to a resource.
3. MOD_SEC: sec:identifier

- sec:identifier is an element for the unique identifier assigned by vendor.

- Syntax

  \[
  <\text{sec:identifier}>%id</\text{sec:identifier}>
  \]

  - %id
    An attribute is the unique identifier assigned by vendor, such as "Cisco Security Advisory ID#50960", HPSBMA01234 etc.
ID: JVNTA06-109A

Title: Oracle Products Contain Multiple Vulnerabilities

Reference: http://www.us-cert.gov/cas/techalerts/TA06-109A.html

<entry>
<title>Oracle Products Contain Multiple Vulnerabilities</title>
<link rel="alternate" type="text/html" href="http://jvn.jp/cert/JVNTA06-109A/">
<id>http://jvn.jp/cert/JVNTA06-109A/</id>
<summary type="text">Oracle products and components are affected by multiple vulnerabilities. </summary>
<published>2006-04-20T11:30+09:00</published>
<updated>2006-04-21T15:00+09:00</updated>
<author>
<name>JVN</name>
<email>jvn@jvn.jp</email>
<uri>http://jvn.jp/</uri>
</author>
<sec:identifier>JVNTA06-109A</sec:identifier>
<sec:references sec:source="CERT" sec:id="TA06-109A">
    http://www.us-cert.gov/cas/techalerts/TA06-109A.html
</sec:references>
</entry>
Reference

- IPA (Information-technology Promotion Agency, Japan)

- JPCERT/CC
  - http://www.jpcert.or.jp/english/

- JVN (JP Vendor Status Notes)
  - http://jvn.jp/ (Japanese)

- JVNRSS (JP Vendor Status Notes RSS) Feasibility Study Site
  - http://jvnrss.ise.chuo-u.ac.jp/jtg/
We propose "JVNRSS" to solve the problems and improve the security information exchange for security administrators. JVNRSS is based on RSS 1.0 and use the field <dc:relation> of Dubline Core as index of grouping security information. This presentation has discussed the specification of JVNRSS and the application, especially the gathering and grouping approach for the security information exchange. Furthermore, we introduce RSS extension of security information exchange.
Thank you

Proposal of RSS Extension
for Security Information Exchange

2006/06/30

Masato Terada
office@jpcert.or.jp
http://jvn.jp/

IPA (Information-technology Promotion Agency, Japan)
JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)