Hitachi update
Hitachi Incident Response Team

2005/10/05
October 2005 FIRST Technical Colloquium
October 01 - 07, 2005 - Buenos Aires, Argentina

Masato Terada, Chief Coordination Designer
Hitachi Incident Response Team, Hitachi Ltd.
& IPA (Information-technology Promotion Agency, Japan)
& JPCERT/CC JVN WG

Contents
1. Japan UPDATE
2. Hitachi UPDATE
Team Member meeting

JPCERT/CC, (NIRT), IIJ, LAC, NTT-CERT and HIRT

1st meeting
April 26, 2005 at Hitachi

2nd meeting
July 14, 2005 at NTT

We try to build more trust & worldwide human network.

JVNRSS starts September 9, 2005
http://jvn.jp/rss/

What is JVN?
JPCERT/CC and IPA are promoting to establish the framework of vulnerability (information) handling in Japan. JVN(JP Vendor Status Notes) is security portal site which is promoted under that framework. "Vendor Status Notes" is similar to "CERT Vulnerability Notes" and follows up IPA/JPCERT Advisories, CERT/CC Advisories (US-CERT Alerts), and NISCC Advisories.

What is JVNRSS?
Summary format for security information exchange. JVNRSS is based on RSS 1.0 and use the field <dc:relation> of Dublin Core as index of grouping security information.
1 Japan Update

JVN RSS format

```
<item rdf:about="URL of vendor information">
  <title>Title</title>
  <link>URL of vendor information</link>
  <description>Outline of Security Information</description>
  <dc:publisher>Vendor Name</dc:publisher>
  <dc:identifier>Information ID</dc:identifier>
  <dc:relation>Relational ID { CVE | CERT-CA | CERT-VU | etc. }</dc:relation>
  <dc:date>Last Updated Date</dc:date>
  <dcterms:issued>Release Date</dcterms:issued>
  <dcterms:modified>Last Updated Date</dcterms:modified>
</item>
```

JVN RSS example

```
  <title>Multiple Vulnerabilities in tcpdump</title>
  <link>http://www.turbolinux.co.jp/security/2004/TLSA-2004-3j.txt</link>
  <description>Multiple Vulnerabilities in tcpdump</description>
  <dc:publisher>Turbolinux</dc:publisher>
  <dc:identifier>TLSA-2004-3</dc:identifier>
  <dc:date>2004-01-22T16:18+09:00</dc:date>
  <dc:creator>security-team@turbolinux.co.jp</dc:creator>
</item>
```

Future work of JVNRSS

Visual Tool for Security Information

- Flash tool for JVNRSS (release September 9, 2005)
  - ticker
  - box
  - etc.

- Flash tool for Status Tracking Notes (work in progress)
  “Status Tracking Notes” is in sharing the public events of time series, which include worm activities, exploit codes releasing and the countermeasure of security incidents.
"Status Tracking Notes" is in sharing the public events of time series, which include worm activities, exploit codes releasing, and the countermeasure of security incidents.
## Japan Update

### JVN Identifier is based on CERT Advisory

**Title**

**Microsoft Windows JPEG にバッファオーバーフローエ**

<table>
<thead>
<tr>
<th>Time (JST)</th>
<th>Event Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004-09-15 09:20</td>
<td>TRTA04-260A</td>
</tr>
<tr>
<td>2004-09-15 09:20</td>
<td>コードインジェクション: 2004年9月7日のセキュリティ更新を解説</td>
</tr>
<tr>
<td>2004-09-15 09:20</td>
<td>Post Date: Thu, 16 Sep 2004 15:20:18 -0700</td>
</tr>
<tr>
<td>2004-09-15 09:20</td>
<td>UN-DEPT JVN-2004-260A</td>
</tr>
<tr>
<td>2004-09-23 03:03</td>
<td>TRTA04-260A: Microsoft Windows JPEG Chocky Streaming Exploit</td>
</tr>
<tr>
<td>2004-09-23 03:03</td>
<td>Post Date: Wed, 22 Sep 2004 11:08:18 -0700 (PDT)</td>
</tr>
<tr>
<td>2004-09-23 03:03</td>
<td>Original JVN-260A: JEDO Remote Exploit</td>
</tr>
<tr>
<td>2004-09-23 03:03</td>
<td>Original JVN-260A: JEDO Remote Exploit</td>
</tr>
</tbody>
</table>
Visual tool for Status Tracking Notes

Future work of JVNRSS

RSS Extension for Security Information Exchange
JVNRSS is proprietary format in Japan.
=> We would like to exchange security information in worldwide.

CVE+ project (Tentative name)
The relationship map between CVE and Japanese Security Information.

CVE-2004-0230
VU#415294
BID10183
XF15886
TA04-111A
NISCC23629

[item rdf:about="http://example.jp/adv1.txt"]
<title>Vulnerability Issues in TCP</title>
<link>http://example.jp/adv1.txt</link>
<dc:relation>TA04-111A</dc:relation>
</item>

[item rdf:about="http://sample.jp/adv2.txt"]
<title>Potential Reliability Issue in TCP</title>
<link>http://sample.jp/adv2.txt</link>
<dc:relation>NISCC23629</dc:relation>
</item>
2 Hitachi Update

HIRT Web site starts September 9, 2005

Japanese: http://www.hitachi.co.jp/hirt/
English: http://www.hitachi.com/hirt/

Security Information Portal Site of Hitachi Group starts...

Japanese: http://www.hitachi.co.jp/hirt/security/
English: http://www.hitachi.com/hirt/security/

JVRRSS Feed of Hitachi Group Security Information

English: Coming soon

Summary of my project of 17th FIRST conference

My project summary
------------------
Project Name: Talking with all participants.
Period: 2005/06/27 - 2005/07/01 (5 days)

Results
Number of registration 328
Number of achievement 152 (46.3%)

Thank you for cooperation to my project
to talk with all participants.

I look forward to meeting FIRST members in Baltimore.
Thank You

HIRT
Hitachi Incident Response Team,

2005/10/05
October 2005 FIRST Technical Colloquium
October 01 - 07, 2005 - Buenos Aires, Argentina

Masato Terada, Chief Coordination Designer
Hitachi Incident Response Team, Hitachi Ltd.