

# 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

**HITACHI**  
Inspire the Next

## Contents

1. Japan UPDATE
2. Hitachi UPDATE

**HITACHI**  
Inspire the Next

## **Team Member meeting**

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

**1<sup>st</sup> meeting**

**April 26, 2005 at Hitachi**

**2<sup>nd</sup> 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.

## 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

```
<item rdf:about="http://www.turbolinux.co.jp/security/2004/TLSA-2004-3j.txt">
  <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:relation>http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0989</dc:relation>
  <dc:relation>http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0055</dc:relation>
  <dc:relation>http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0057</dc:relation>
  <dc:relation>http://www.turbolinux.co.jp/security/TLSA-2003-14j.txt</dc:relation>
  <dc:date>2004-01-22T16:18+09:00</dc:date>
  <dc:creator>security-team@turbolinux.co.jp</dc:creator>
</item>
```

Copyright © Hitachi, Ltd. 2005. All rights reserved. 4

## Future work of JVN RSS

### Visual Tool for Security Information

Flash tool for JVN RSS (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.

Copyright © Hitachi, Ltd. 2005. All rights reserved. 5

**Visual tool for JVNRSS**

Copyright © Hitachi, Ltd. 2005. All rights reserved. 6

**“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.**

Copyright © Hitachi, Ltd. 2005. All rights reserved. 7

JP Vulnerability Notes - Status Tracking Note TRTA04-260A - Microsoft Internet Explorer

Status Tracking Notes

TRTA04-260A ← [JVN Identifier is based on CERT Advisory](#)

Microsoft Windows JPEG にバッファオーバーフロー ← [Title](#)

時系列イベント ↓ [Time \(JST\)](#) ↓ [Event Information](#)

日時 (JST)	内容
2004-09-15 05:22	<a href="#">マイクロソフト: セキュリティ情報 2004 年 9 月のセキュリティ情報</a> #Post-Date: Tue, 14 Sep 2004 13:22:15 -0700
2004-09-17 04:58	US-CERT <a href="#">TA04-260A</a> #Post-Date: Thu, 16 Sep 2004 15:58:16 -0400
2004-09-23 03:38	Full-Disclosure "Microsoft Windows MS04-028 JPEG Overflow Shellcoded Exploit" #Cid: ms04-28-cmd.c #Tested: Windows XP + SP1 #Post-Date: Wed, 22 Sep 2004 11:38:18 -0700 (PDT)
2004-09-23 15:22	Bugtraq "NEW GDI+ JPEG Remote Exploit" #Cid: JpegOfDeath.c #Tested: Windows XP + SP1 #Post-Date: 23 Sep 2004 06:22:54 -0000
2004-09-23 23:55	I
2004-09-24 13:49	ISSI4K <a href="#">Microsoft の JPEG 処理 (GDI+) における悪用</a> を Web 公開 #ISSXPU: <a href="#">Network Sensor 22.31</a> #Last-Modified: Fri, 24 Sep 2004 04:49:46 GMT

**Notice: Some events are omitted.**

## Visual tool for Status Tracking Notes

Status Tracking Notes

TRTA05-221A Microsoft Windows and Internet Explorer Vulnerabilities

TRTA05-210A Cisco IOS IPv6 Vulnerability

TRTA05-194A Oracle 製品群に対する脆弱性

TRTA05-193A Microsoft Windows、Internet Explorer および Word における脆弱性1234567890ABCDEF

TRTA05-180A VERITAS Backup Exec Remote Agent の脆弱性を対象とする侵害活動

TRTA05-189A 「トロイの木馬」送付メールの流布

TRTA05-102A Microsoft Windows コンポーネントに存在する複数の脆弱性

TRTA05-165A Microsoft Windows および Internet Explorer に存在する複数の脆弱性

TRTA05-039A Microsoft Windows コンポーネントに存在する複数の脆弱性

TRTA05-136A Apple の Mac OS X に複数の脆弱性

TRTA05-117A オラクル製品に複数の脆弱性

TRTA05-012A Microsoft Windowsでアイコンおよびカーソルの処理に複数の脆弱性

TRTA05-026A Cisco IOS にサービス運用妨害 (DoS) 攻撃を受けける複数の脆弱性

TRTA05-012B Microsoft WindowsでHTML HelpのActiveXコントロールがロードされる脆弱性

TRTA04-041A Microsoft Windows ASN1 ライブラリに脆弱性

TRTA04-293A Microsoft Internet Explorer に複数の脆弱性

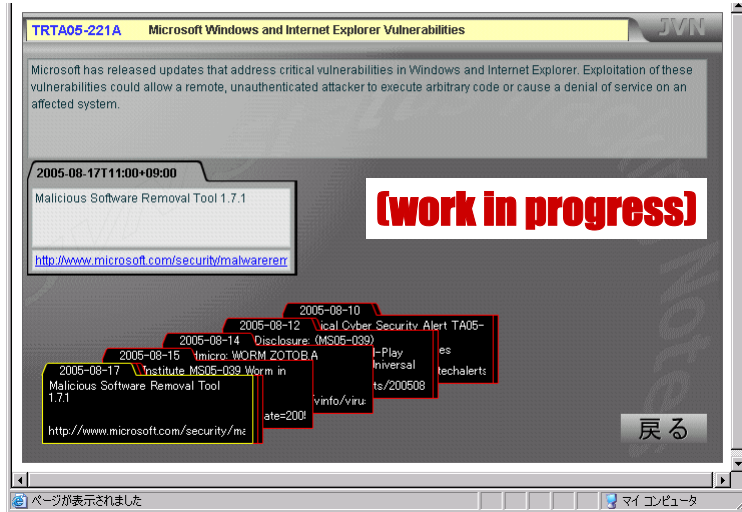
TRTA04-245A オラクル製品に複数の脆弱性

**(work in progress)**

ページが表示されました

マイコンピュータ

## Visual tool for Status Tracking Notes



## Future work of JVN RSS

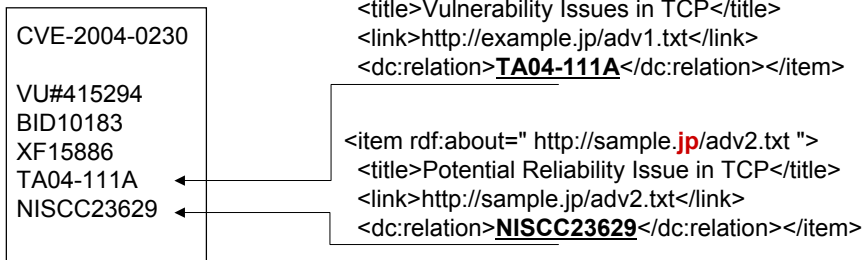
### RSS Extension for Security Information Exchange

JVN RSS 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.



## 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/>

### JVNRSS Feed of Hitachi Group Security Information

Japanese: <http://www.hitachi.co.jp/hirt/security/index.rdf>  
English: **Coming soon**

HIRT Logo



## Ending

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.