

## Information Security Early Warning Partnership

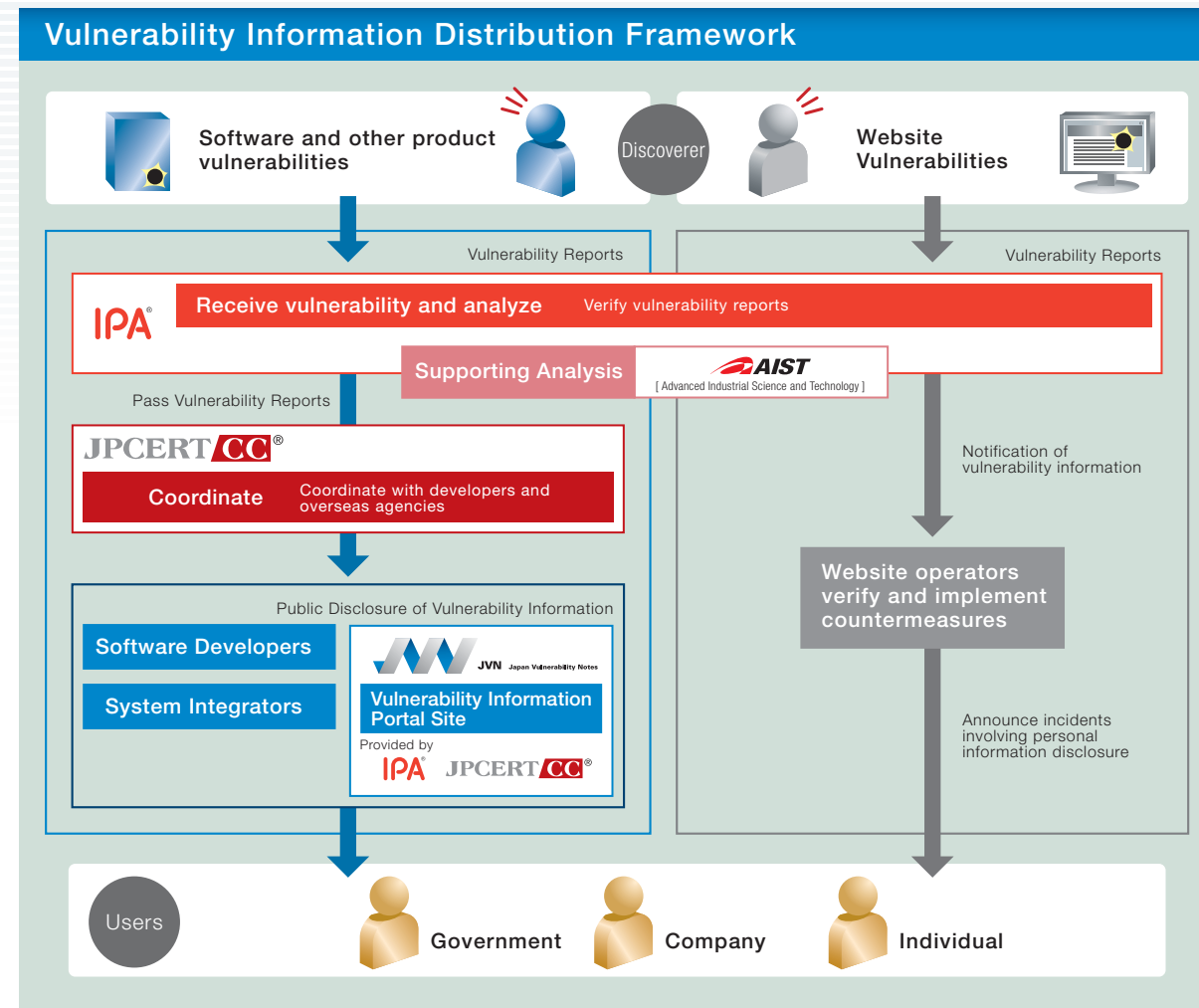
[ In service from July 2004 in accordance with the METI\* notification ]

\*METI = Ministry of Economy, Trade and Industry

The Information Security Early Warning Partnership strengthens the communication between vulnerability reporters and software developers and website operators. The information on vulnerabilities in software products is first reported to IPA, then passed to JPCERT/CC. JPCERT/CC specifies the affected software products and coordinates with developers. The framework is designed to protect users from computer virus attacks and unauthorized access, disclosure of private information, and failure of IT systems by preventing vulnerability information disclosure before any remediations are available. JVN publishes the vulnerability details with developers' notes to act against the vulnerability.



**JVN** Japan Vulnerability Notes



Vulnerability Information Portal Site

<http://jvn.jp/>

A vulnerability Knowledge-base assisting software and other products developers enhance security for their products and customers

Copyright © 2007 IPA and JPCERT/CC. All rights reserved.  
 The IPA logo is a registered trademark of the Information-technology Promotion Agency, Japan. The JPCERT/CC logo is a registered trademark of the JPCERT Coordination Center.  
 All other company names and product names are trademarks or registered trademarks of their respective owners.

**IPA** IT Security Center  
 Information-technology Promotion Agency, Japan

IT Security Center  
 Information-technology Promotion Agency, Japan  
 16th Floor, Bunkyo Green Court Center Office  
 2-28-8 Hon-Komagome, Bunkyo-ku, Tokyo 113-6591 Japan  
 Tel: +81-3-5978-7527 Fax: +81-3-5978-7518  
<http://www.ipa.go.jp/security/>

**JPCERT/CC**

Japan Computer Emergency Response Team  
 Coordination Center  
 11th Floor, Hirose Bldg.  
 3-17 Nishiki-cho, Kanda, Chiyoda-ku, Tokyo 101-0054 Japan  
 Tel: +81-3-3518-4600 Fax: +81-3-3518-4602  
<http://www.jpccert.or.jp/>





# JVN Japan Vulnerability Notes

## Definitive Vulnerability Knowledge-base for Information Systems

Today's social and economic infrastructure largely depends on information technology. In order to keep such infrastructure safe and reliable, it is necessary not only to prepare for natural disasters and system failures, but also to implement security measures against cyber attacks, computer viruses, and unauthorized access via the Internet.

Addressing the vulnerability is important among other security measures. System administrators and integrators must collect and sort vulnerability information reports every day, assess risks, understand the nature of the problems, and take appropriate actions.

To assist the people engaged in such operations, IPA and JPCERT/CC jointly run a vulnerability information portal site, Japan Vulnerability Notes (JVN), to provide vulnerability information regarding software and other products. We will continue providing security information to IT users and products developers.

### JVN : Providing reliable vulnerability information

Under Information Security Early Warning Partnership, IPA receives private vulnerability reports and JPCERT/CC coordinates with developers to prepare patches or remedies. JVN provides the information such as:

- Solution
- Vulnerability Analysis by JPCERT/CC
- Vendor Notes

Vulnerability information, especially on Open Source Software (OSS), often affects multiple products. In such a case, JVN provides notes from those vendors affected.

### Chronological Information that Supports Vulnerability Remediation Process

Records of security events are useful when planning the vulnerability remediation process.

We provide "Status Tracking Notes", the list of relevant events, for some vulnerability information on a trial basis. Records contain exploit code availability, related incidents observed, and availability of fixes.



[JVN Home]

● **Critical**  
Indicated when urgent action is necessary.

● **Products Affected**  
Lists the systems, products, names of libraries, and versions affected.

● **Solution**  
Details available solutions and workarounds.

● **Vendor Notes**  
Links to the developer's page.

### [Vulnerability Report]



● **Vulnerability Analysis by JPCERT/CC**  
Provides the vulnerability analysis by JPCERT/CC

### [Chronological Information]



The English version of JVN will be released in spring 2008.

### RSS Feeds and support tools

We provide JVN updates in RSS (RDF\* Site Summary) format. These updates are readily available using an RSS reader. This enables system administrators and integrators to rapidly collect vulnerability information and solutions.

We also provide tools for displaying JVN updates on your website. (This tool requires Adobe Flash 7.0 or higher for a plug-in.)

\*RDF: Resource Description Framework



Hitachi HIRT\* uses this tool to automatically display JVN updates.  
\*Hitachi Incident Response Team

### JVN iPedia

Vulnerability Countermeasure Information Database

JVN iPedia is an information database that stores summary and countermeasure information on vulnerabilities in Japanese software and other products posted on JVN. In the six months following its public release in April 2007, iPedia catalogued 4,100 vulnerabilities. JVN iPedia is equipped with search functions (keyword search, product search, and severity scoring based on CVSS\*) and RSS feeds, which provides the accumulated data in a comprehensive manner.

\*CVSS: Common Vulnerability Scoring System



Provides vulnerability countermeasure information collected and accumulated every day.