

Summit Days

Structure and numbering of JVN, and Security content automation framework

November 14, 2012

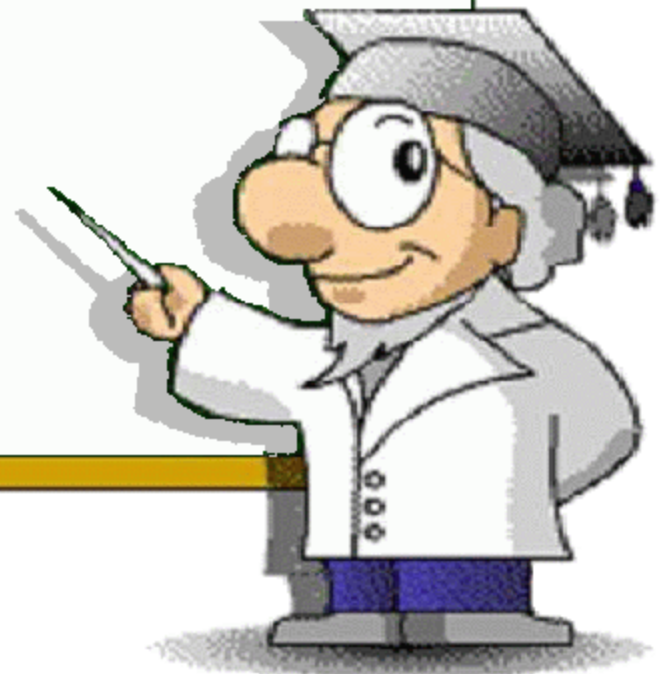
**Masato Terada
IT Security Center, IPA**



- **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

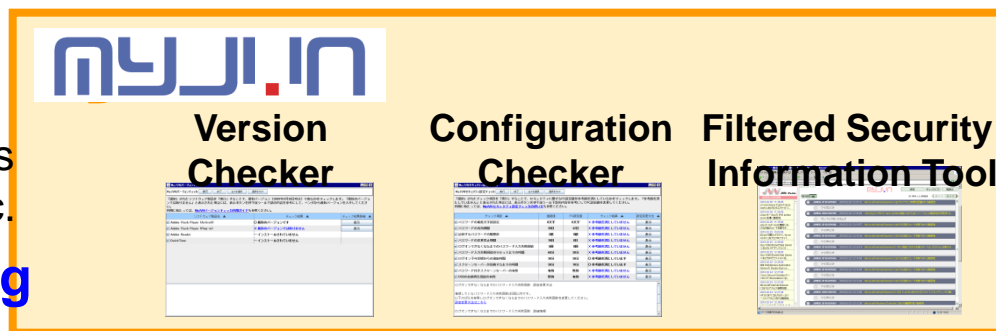


structure and numbering of jvn.

= (**Internationalization** + **Localization**) x **Machine readable**

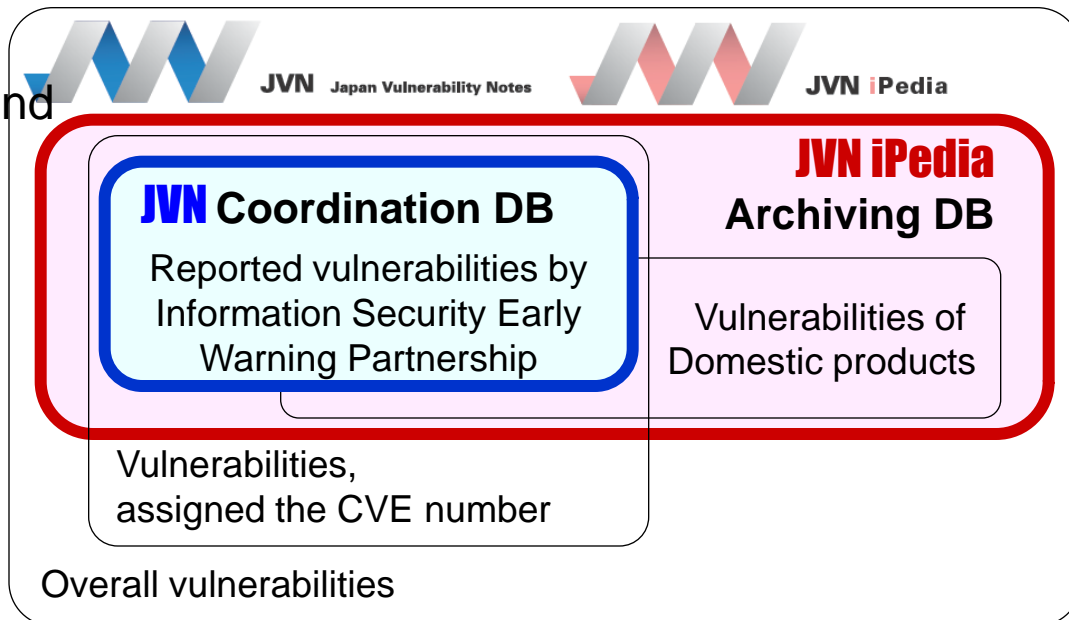
- **MyJVN**

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”



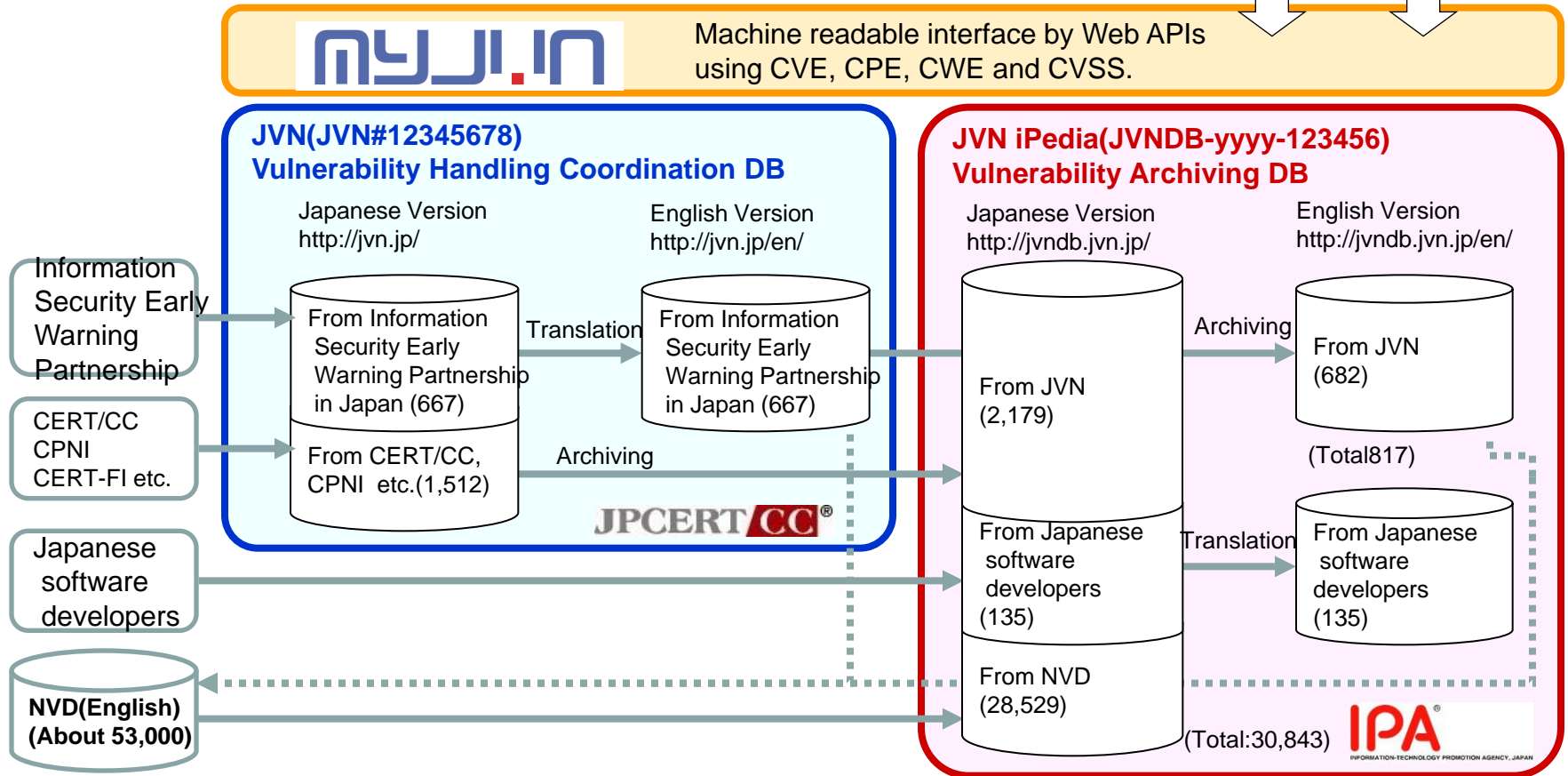
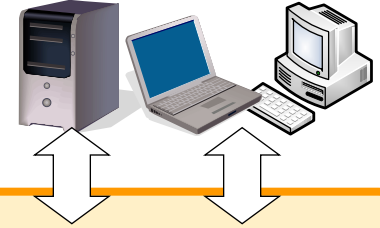
- **JVN iPedia (Vulnerability archiving DB)**

Providing countermeasure information database for covering overall vulnerabilities

structure and numbering of jvn.

Structure

- Flow of data exchange between DBs



2012 3th Quarter

structure and numbering of jvn.

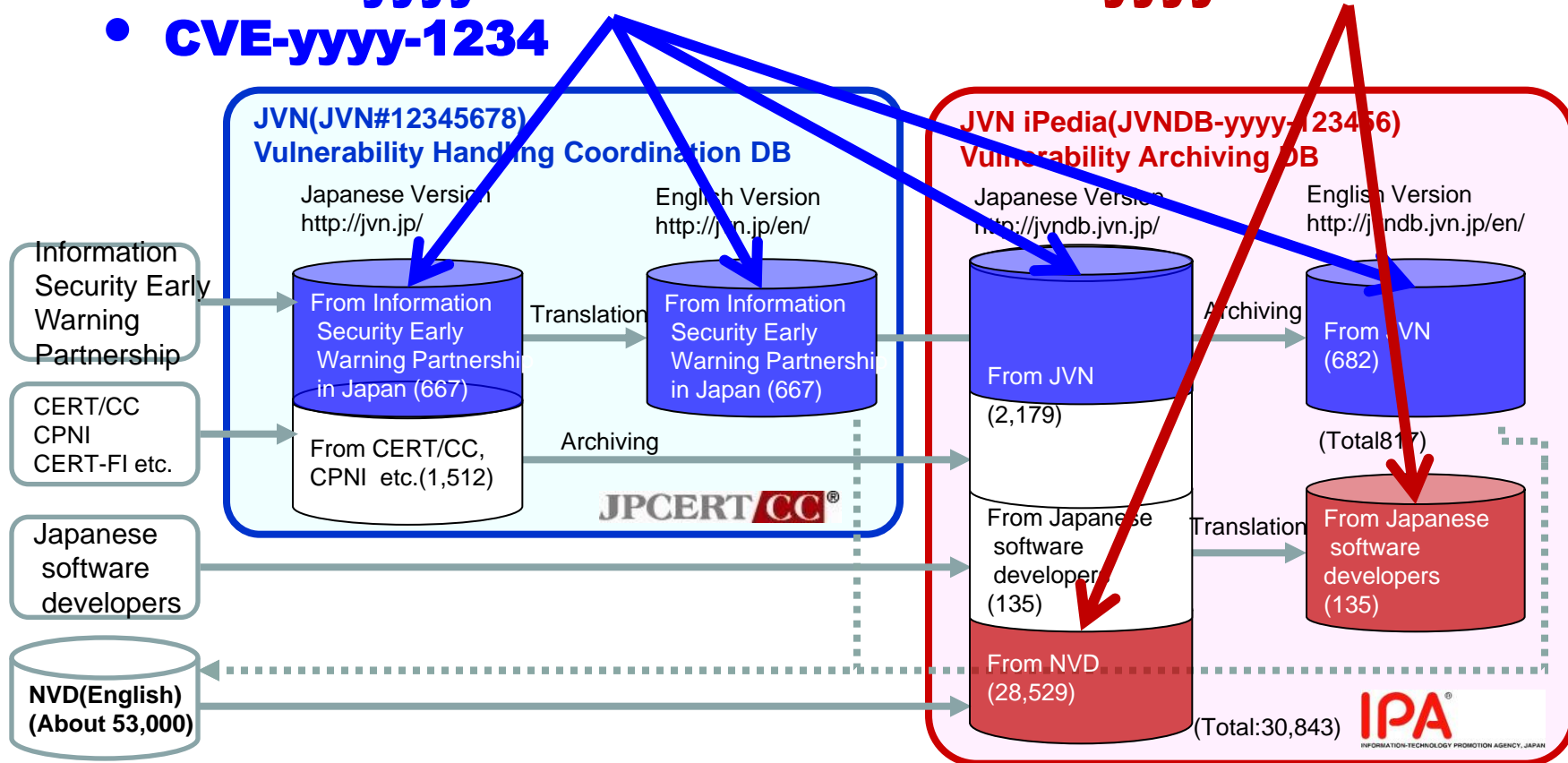
Numbering

Assign three identifiers

- **JVN#12345678**
- **JVNDB-yyyy-123456**
- **CVE-yyyy-1234**

Assign two identifiers

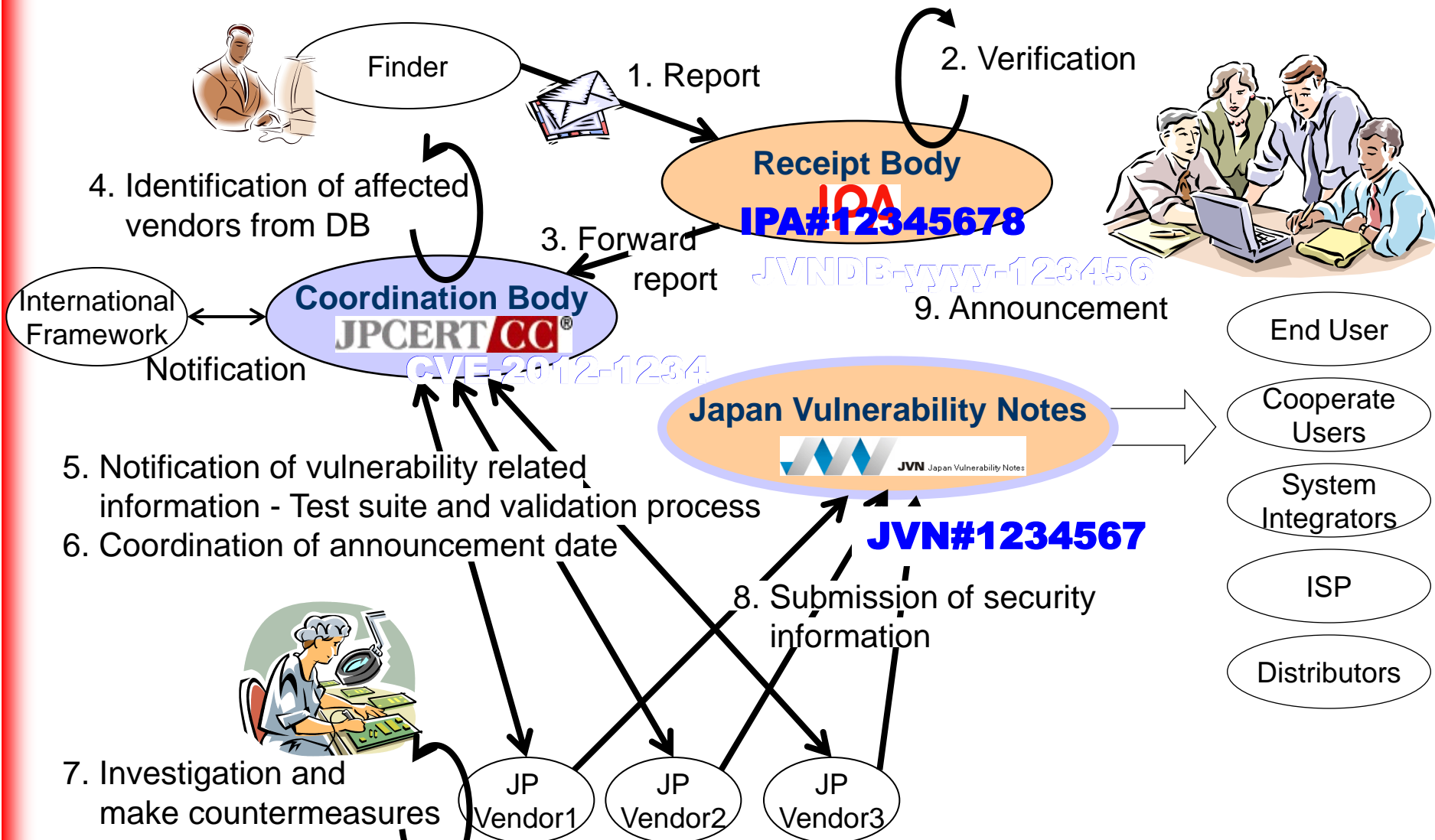
- **JVNDB-yyyy-123456**
- **CVE-yyyy-1234**



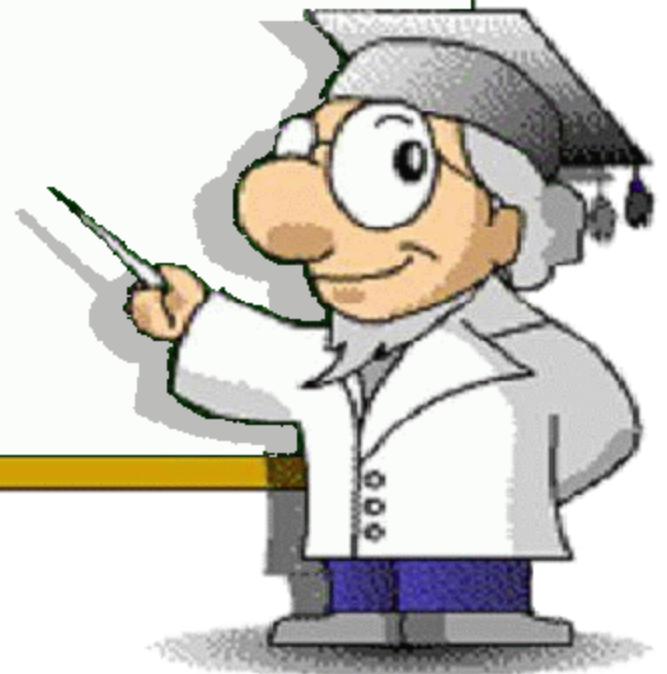
2012 3th Quarter

structure and numbering of jvn.

Numbering and Vulnerability Reporting



- Structure and numbering of JVN
- **JVN Security Content Automation Framework**
- MyJVN project



= (JVN + JVN iPedia) x MyJVN

= MyJVN framework

- To enable application developers to use data through open interface
 - Adoption for common enumeration and specifications
- To establish global JVN
 - Internationalization as vulnerability reference source
 - Localization as vulnerability reference source (focus to Japanese region)

JVN Security Content Automation Framework (aka. MyJVN framework) has adopted SCAP.

related activities (phase 1).

JVN Security Content Automation Framework



2003 | **2004** | **2005** | **2006** | **2007** | **2008** | **2009** | **2010** | **2011** | **2012**

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

- ▲ Jul 7, 2004: Information security early warning partnership
- ▲ Jul 8, 2004: **JVN (aka. Vuln. handling coordination DB)** <http://jvn.jp/>

- ▲ 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).

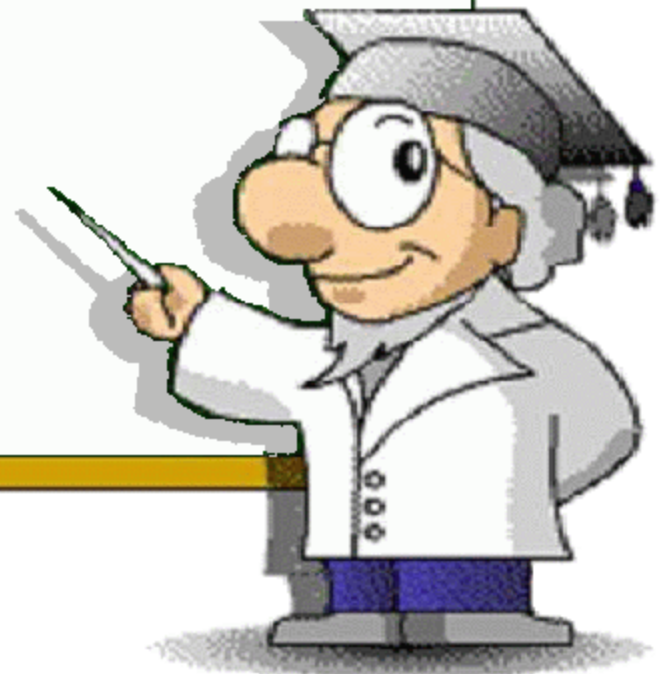
JVN Security Content Automation Framework



2008 | **2009** | **2010** | **2011** | **2012** | **2013** | **2014** | **2015** | **2016** | **2017**

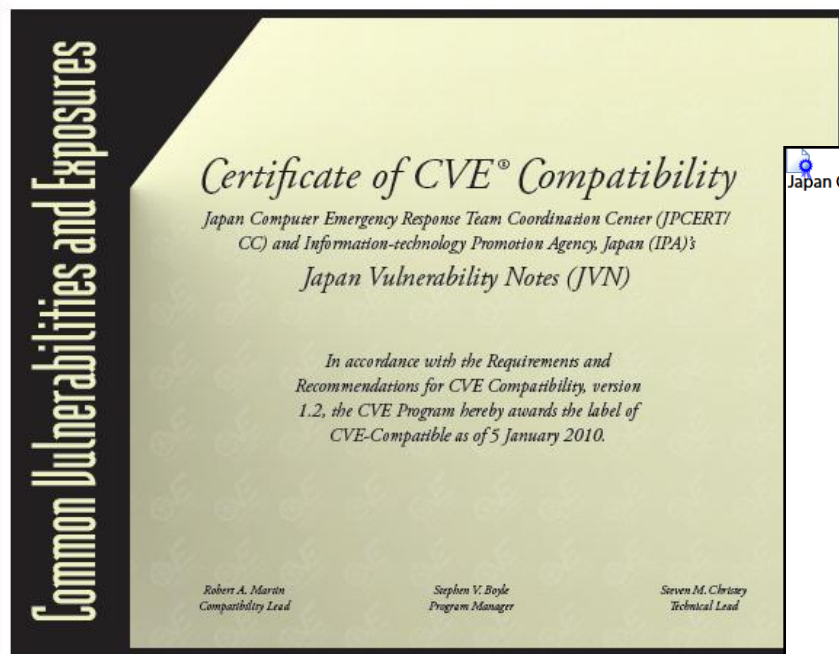
- ▲ Sep 2008: MyJVN project started
- ▲ Oct 2008: JVN iPedia extension (**Adopted CPE**)
- ▲ Oct 2008: **MyJVN Filtered vulnerability information tool** (**Adopted CPE**)
 - ▲ Nov 2009: **MyJVN Version Checker (VC)** (**Adopted CPE and OVAL**)
 - ▲ Dec 2009: **MyJVN Security Configuration Checker (SCC)** (**Adopted OVAL, CCE and XCCDF**)
 - ▲ Jan 2010: **JVN, JVN iPedia** and **MyJVN** (**CVE-Compatible**)
 - ▲ Jan 2010: CVSS V2.0 Calculator [AR][EN][FR][DE][JA][KO][ES]
 - ▲ Feb 2010: **MyJVN API** (**Filtered information service API**)
 - ▲ Jun 2010: **MyJVN - VRDA** collaboration
 - ▲ Mar 2011: **MyJVN VC** and **MyJVN SCC** (**OVAL Adopter**)
 - ▲ Aug 2012: **MyJVN API** (**SCAP collaboration service API**)

- Structure and numbering of JVN
- JVN Security Content Automation Framework
- **MyJVN project**



- **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)



Japan Computer Emergency Response Team Coordination Center

JPCERT/CC®



プレスリリース
2010年6月24日
一般社団法人 JPCERT コーディネーションセンター

JPCERT/CC、国内初の CNA (CVE Numbering Authority) に認定
～第三者調整機関としては米国 CERT/CC に次いで 2 組織め～

一般社団法人 JPCERT コーディネーションセンター(東京都千代田区、代表理事 歌代 和正、以下「JPCERT/CC」といいます。)は、CVE(Common Vulnerabilities and Exposures)¹を管理運営する米国 MITRE 社が 2010 年 6 月 23 日付け²で JPCERT/CC を CNA(CVE Numbering Authority, CVE 採番機関)³に認定したと発表しました。

- **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 API	Information-technology Promotion Agency, Japan (IPA)	Vulnerability Assessment and Configuration Management	Japan	Definition Repository	Declaration
MyJVN Security Configuration Checker	Information-technology Promotion Agency, Japan (IPA)	Configuration Management	Japan	Definition Evaluator	
MyJVN Version Checker	Information-technology Promotion Agency, Japan (IPA)	Vulnerability Assessment	Japan	Definition Evaluator	

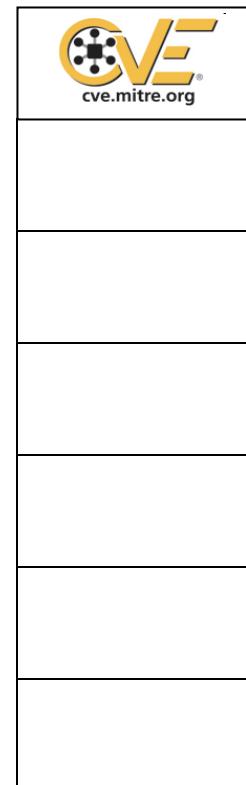
- **Technical View**

- 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



- **JVN**

- 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)



jvn - vulnerability notes (vn).

<http://jvn.jp/en/>



- VN includes a list of JP product vendors who may be affected by the vulnerability.



Published:2007/12/13 Last Updated:2008/08/20

JVN#80057925
Cross-site scripting vulnerability in Apache HTTP Server "mod_imap" and "mod_imagemap"

Overview

mod_imap an

JVN#12345678 Server are vulnerable to cross-site scripting.

Products A

- ♦ Apache H
- ♦ Apache H

Title

Overview

Impact

Vendor Status

Reference

Revisions

There are five categories as Status.

- Unknown
- Vulnerable (Completed investigation)
- Vulnerable (Under investigation)
- Not Vulnerable (Completed investigation)
- Not Vulnerable (Under investigation)

image mapping

		Last Update	Vendor Notes
Hitachi	Vulnerable	2007/12/13	
NEC Corporation	Not Vulnerable, investigating	2007/12/13	
Century Systems Co., Ltd.	Not Vulnerable, investigating	2007/12/13	
FUJITSU LIMITED	Vulnerable, investigating	2008/01/17	
Canon Inc.	Not Vulnerable	2008/08/20	

Vendor Link

The Apache Software Foundation [Apache 2.2 Security Vulnerabilities CVE-2007-5000](#)

jvn - vulnerability notes (vn).

<http://jvn.jp/en/>

IPA



JVN Japan Vulnerability Notes

http://jvn.jp - Japan Vulnerability Notes - Microsoft Internet Explorer

Date Last Updated: March 14, 2011

JVN Japan Vulnerability Notes

JVN English Site Open Past Announcements

Recent Vulnerability Notes

[RSS](#)

JVN#01635457:	e107 vulnerable to cross-site scripting [March 14, 2011 12:00]
JVN#81294135:	IBM Tivoli vulnerable to denial-of-service (DoS) [March 10, 2011 12:00]
JVN#73162541:	OTRS vulnerable to OS command [March 10, 2011 12:00]
JVN#97334690:	IBM Lotus vulnerable to denial-of-service (DoS) [March 04, 2011 16:00]
JVN#26301278:	IBM WebSphere Application Server vulnerable to denial-of-service (DoS) [March 04, 2011 16:00]

JVN

- HOME
- What is JVN ?
- Instructions
- List of Vulnerability Report
- VN_JP

cve.mitre.org

JVN

- HOME
- What is JVN ?
- Instructions
- List of Vulnerability Report
- VN_JP
- TRN

http://jvn.jp - JVN#88991166: SEIL Series routers vulnerable to buffer overflow - Microsoft Internet Explorer

Published: 2011/02/28 Last Updated: 2011/02/28

JVN#88991166

SEIL Series routers vulnerable to buffer overflow

Overview

SEIL Series routers contain a buffer overflow vulnerability.

Products Affected

- SEIL/x86 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

- HOME
- What is JVN ?
- Instructions
- List of Vulnerability Report
- VN_JP
- TRN
- JVN iPedia
- JVNJS/RSS
- Vendor List
- Contact

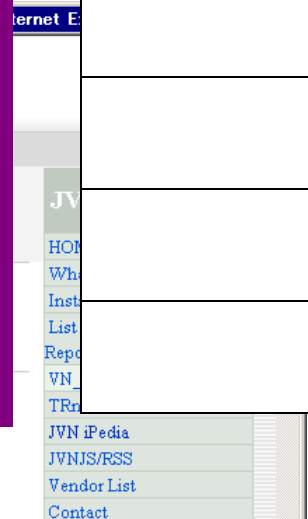
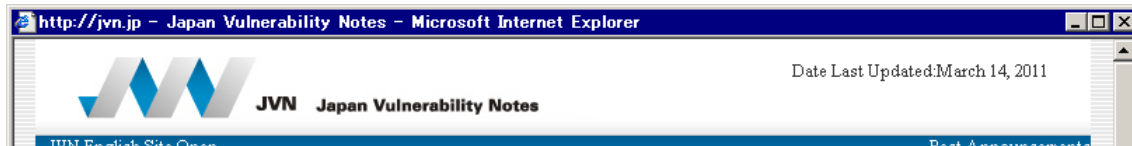
jvn - vulnerability notes (vn).

<http://jvn.jp/en/>

IPA



JVN Japan Vulnerability Notes



- SEIL/x86 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 - status tracking notes (trnotes).

<http://jvn.jp/en/>



JVN Japan Vulnerability Notes

- The purpose of TRnotes is in sharing the events of time series. The event information is based on public information.



Published: 2008-07-20T10:29+00:00 Last Updated: 2008-08-31T04:54+00:00

TRTA08-190B

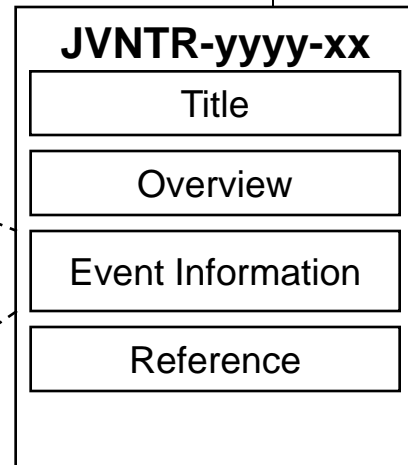
Multiple DNS implementations vulnerable to cache poisoning

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

Date (UTC)	Description
2008-08-24	ICANN Domain Name Security Paper Released ICANN's strategic and operating plans call for ICANN to be operationally ready to deplete DNSSEC at the root level and work with relevant stakeholders to determine how this should be implemented.
	Office of Management and Budget M-08-23: Securing the Federal Government's Domain Name System Infrastructure (Subsequent Draft Agency Plans Due by September 5, 2008) This memorandum describes existing and new policies for deploying Domain Name System



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.



- **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.





Information

Listed on Feb 14, 2011 JVN iPedia Registration Status for 2010 4Q(Oct. - Dec.)
http://www.ipa.go.jp/security/english/vuln/JVNiPedia2010q4_en.html

Most Popular Vulnerabilities on JVN iPedia (2011/03/13 - 2011/03/19)

1. **JVNDB-2011-000019**
OTRS vulnerable to OS comman
2. **JVNDB-2011-000017**
IBM WebSphere Application Se
3. **JVNDB-2011-000020**
IBM Tivoli vulnerable to denial-of

Database Search

JVNDB-2009-000018

Ichitaro series buffer overflow vulnerability

Overview

The "Ichitaro" series word processing software contains a buffer overflow vulnerability.

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

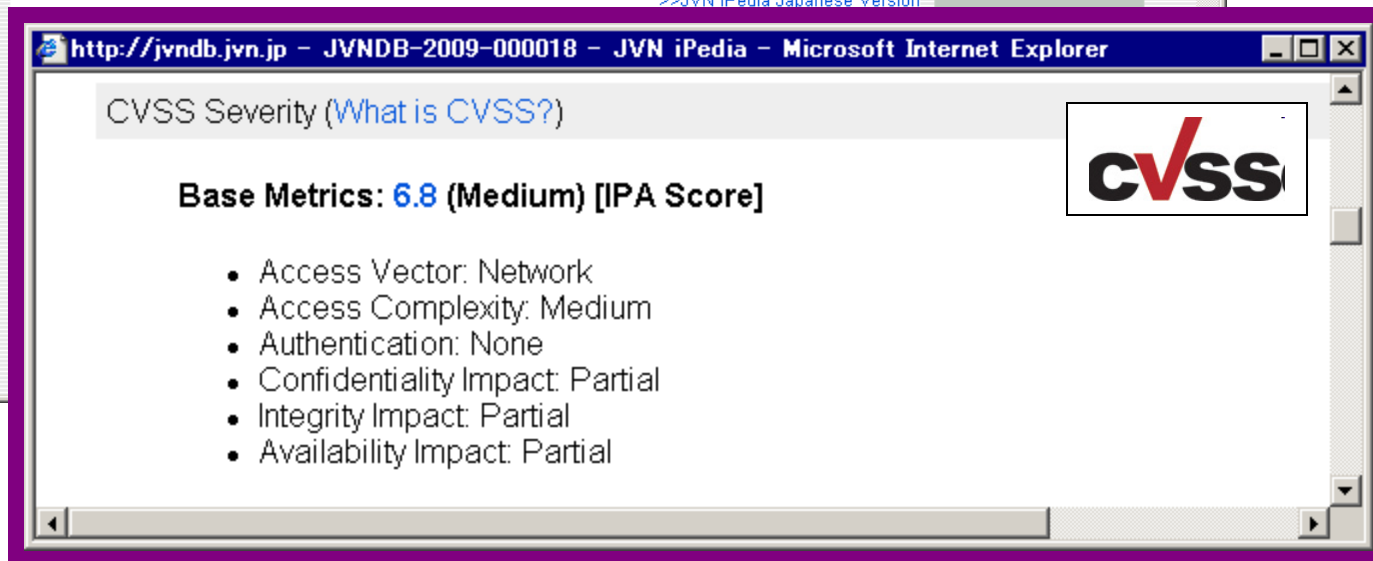
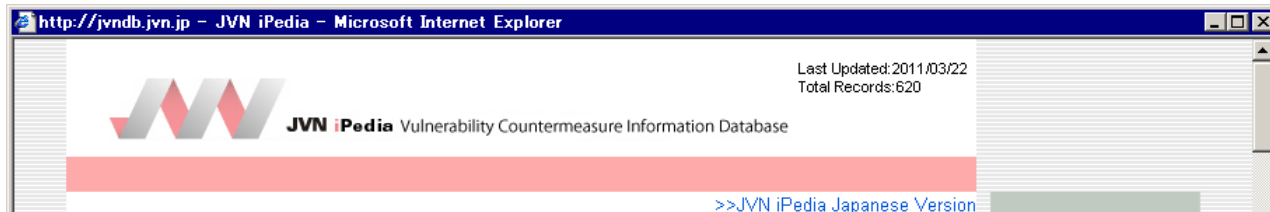
The "Ichitaro" series word processing software, from JustSystems Corporation, contains an issue in the reading of Rich Text Files resulting in a

CVE
cve.mitre.org

CPE
common platform enumeration

CVSS

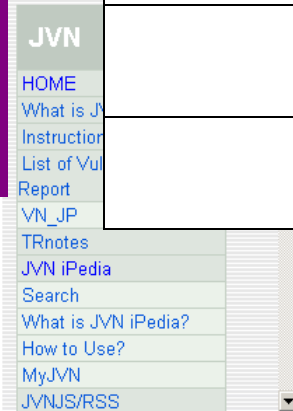
CWE



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





http://jvndb.jvn.jp - JVN iPedia - Microsoft Internet Explorer

Last Updated: 2011/03/22
Total Records: 620

JVN iPedia Vulnerability Countermeasure Information Database

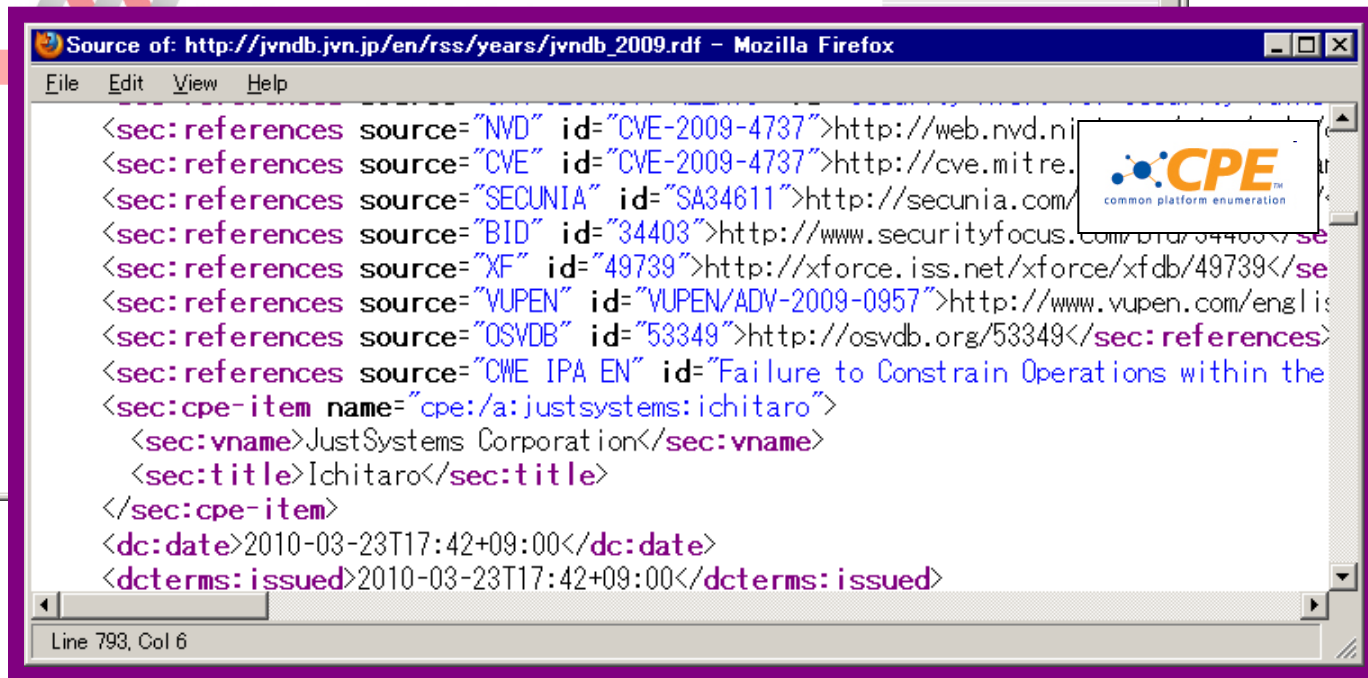
References

1. JVN : [JVN#33846134](#)
2. IPA SECURITY ALERTS : [Security Alert for Security Vulnerability in the Ichitaro Series](#)
3. National Vulnerability Database (NVD) : [CVE-2009-4737](#)
4. Common Vulnerabilities and Exposures (CVE) : [CVE-2009-4737](#)
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

Search
What is JVN iPedia?
How to Use?
MyJVN
JVNJS/RSS



**XML format
= RSS1.0+mod_sec**

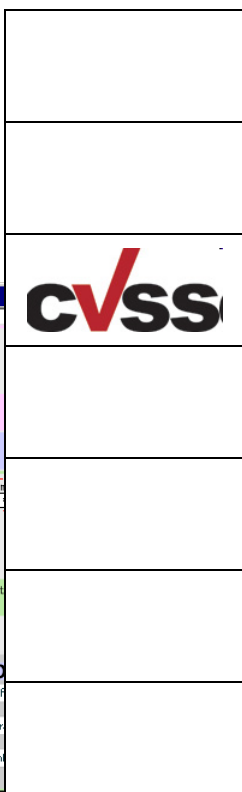
Update	RDF (Update: 2011/03/21) (PGP sig)			
Yearly Data	2011 (PGP sig)	2010 (PGP sig)	2009 (PGP sig)	2008 (PGP sig)
	2007 (PGP sig)	2006 (PGP sig)	2005 (PGP sig)	2004 (PGP sig)
	2003 (PGP sig)	2002 (PGP sig)		
	What is JVND BRSS?			



● CVSS V2.0 Calculator

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

The screenshot displays the CVSS 2.0 Calculator web application interface. It features a navigation menu on the left with options like Home, main, JVN RSS Activity, CVE+, CVSS, RSS_dir, SIG_rdf, TRnotes, XSL_swf, Specification, JVNJS, JVN RSS, RSS_mod_sec, VULDEF, Tool, toolbox, Document, docbox, and Related Site. The main content area shows a 'CVSS 2.0' calculator for a 'CVE-9999-9999-Example'. It includes three score gauges: Base Score (10.0), Temporal Score (7.3), and Environmental Score (7.6), along with an Overall Score (7.6). The interface also displays detailed calculation formulas for Base Score, Temporal Score, Adjusted Impact, Adjusted Base, Adjusted Temporal, and Environmental Score. A 'BASE SCORE' table lists metrics like Access Vector (AV: N), Access Complexity (AC: L), Authentication (Au: N), Confidentiality Impact (C: C), Integrity Impact (I: C), and Availability Impact (A: C). A 'TEMPORAL SCORE' table lists metrics like Exploitability (E: POC), Remediation Level (RL: TF), and Report Confidence (RC: UC). An 'ENVIRONMENTAL SCORE' table lists metrics like Collateral Damage Potential (CDP: L), Target Distribution (TD: H), Confidentiality Requirement (CR: M), Integrity Requirement (IR: M), and Availability Requirement (AR: H). The interface includes buttons for 'Reset Scores', 'Update Scores', 'Reset', and 'Calculate'.



cvss calculator.

<http://jvndb.jvn.jp/en/cvss/>



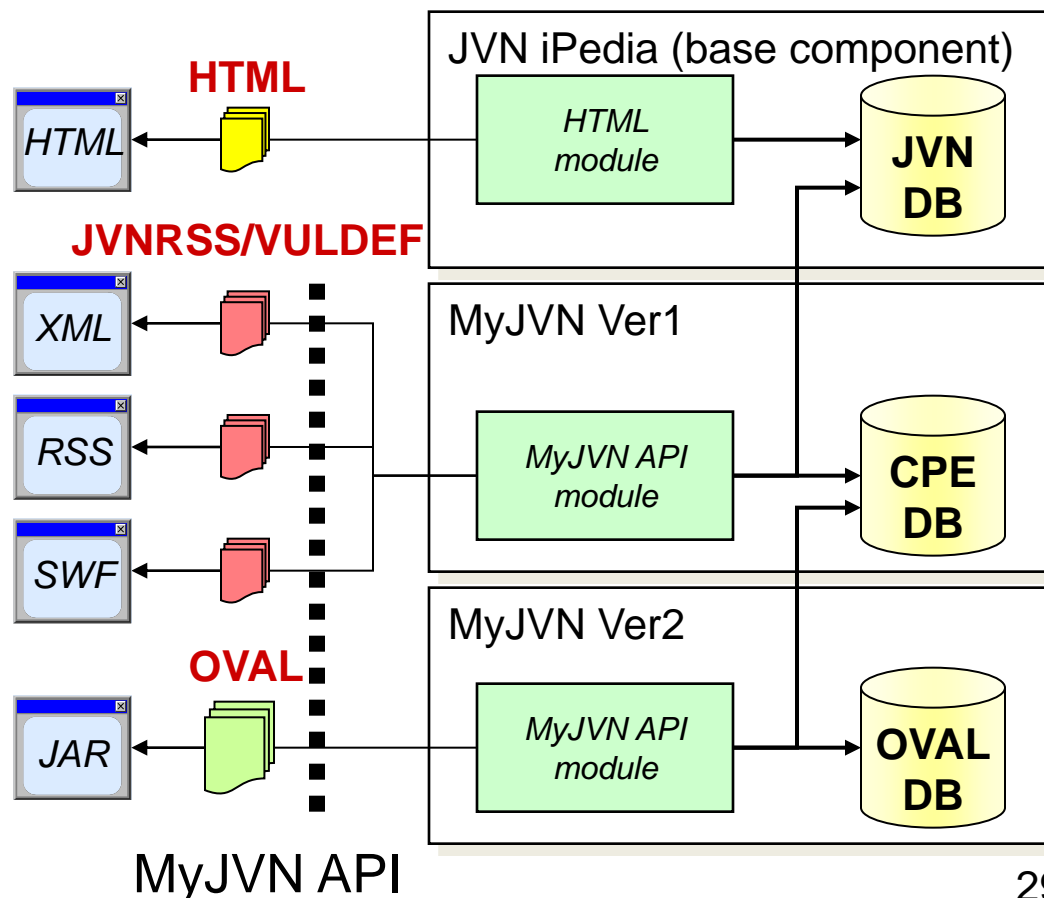
CVSS V2.0 Calculator loads parameter XML file such as Arabic, English and etc.

- **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



- **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.

<http://jvndb.jvn.jp/en/apis/>

IPA

myjvni

- **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**

- <http://jvndb.jvn.jp/myjvn?method=getVulnDetailInfo&vulnId=JVND-2009-000004&lang=en>

filtered information service api.

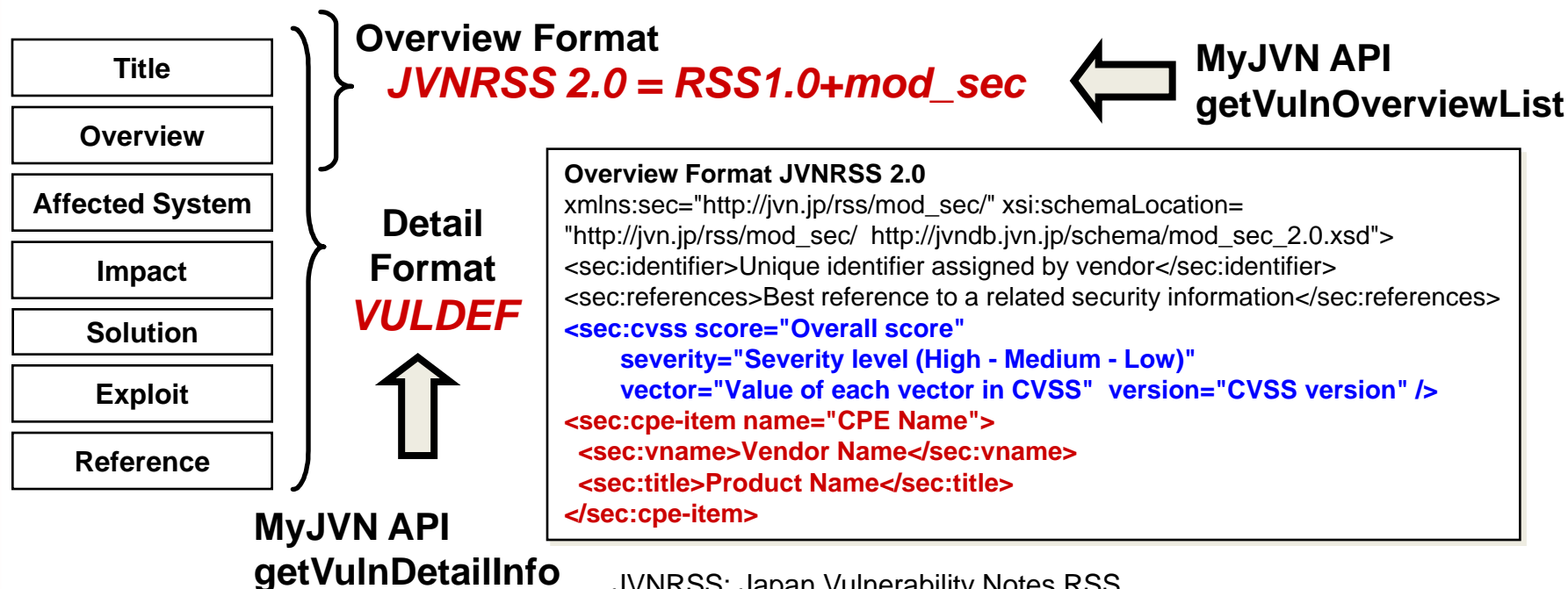
<http://jvndb.jvn.jp/en/apis/>

IPA

情報セキュリティ

- XML formats

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



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.

http://jvndb.jvn.jp/en/apis/

IPA

情報セキュリティ

MyJVN - API: getVendorList - Windows Internet Explorer
http://jvndb.jvn.jp/en/apis/getVendorList.html
MyJVN CPE Search(ja)

Last Updated: 2010/02/25

JVN iPedia Vulnerability Countermeasure Information Database

MyJVN >> API >> getVendorList

[Japanese]

getVendorList

Getting on the vendor list in JVN ver 1.0

This method gets the vendor list by the followed filtering parameters.
XML schemaLocation="http://jvndb.jvn.jp/schema/results_3.0.xsd"

Sample Queries

- Default query
- Get XML result for a given CPE {vendor} field: 'micro'.
- Get XML result for a given CPE {vendor} field: 'micro' and initial 'n' character.

Reset Submit

Parameter name	Description	Parameter Value
method	Method name of API	getVendorList
startItem	Start position of items	<input type="text"/> Integer (1 - The item number of results)
maxCountItem	Maximum number of items	<input type="text"/> Help
cpeName	CPE vendor name (cpe/{vendor})	<input type="text"/> Help
keyword	Keyword search for a vendor by name	<input type="text"/> Help
lang	Language (Japanese/English)	<input checked="" type="radio"/> ja: Japanese <input type="radio"/> en: English
xsl	Applying XSL to XML (Enable/Disable)	<input type="text"/> 1:Enable 0:Disable (Under Construction)

Request and Response

Copyright © 2007-2010 IPA. All rights reserved.

JVN

- HOME
- What is JVN ?
- Instructions
- List of Vulnerability
- Report
- VN_JP
- TRnotes
- JVN iPedia
- Search
- What is JVN iPedia?
- How to Use?
- MyJVN
- JVNJS/RSS
- Vendor List
- Contact

VE
COMPATIBLE

- **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**

- <http://jvndb.jvn.jp/myjvn?method=getOvalList&platform=cpe:/o:microsoft:windows-nt:vista>

- **Get list of XCCDF configuration**

- <http://jvndb.jvn.jp/myjvn?method=getXccdfList>

- **Get Data of OVAL definition**

- <http://jvndb.jvn.jp/myjvn?method=getOvalData&ovalId=oval:jp.jvn.jvndb.v1.oval:def:7>

- **Get Data of XCCDF configuration**

- <http://jvndb.jvn.jp/myjvn?method=getXccdfCheckList&benchmarkId=WindowsXP-IPA-2009>

Filtered security information for your system
 MyJVN Filtered Security Information Tool

JVNDI-2008-000009	2009.04.08 11:33:40
Apple, Inc.	
Apple Mac OS X	
Apple Mac OS X Server	
JVNDI-2007-000817	2009.02.10 11:32:40
Adobe Systems, Inc.	
Adobe Flash Player	

Improvement of the keeping the secure configuration on your PC
 MyJVN Configuration Checker

チェック項目 ▲	推奨値
<input checked="" type="checkbox"/> パスワードの最低文字数設定	8文字
<input checked="" type="checkbox"/> パスワードの有効期間	10日
<input checked="" type="checkbox"/> 記録されたパスワードの総数	2回
<input checked="" type="checkbox"/> パスワードの変更までの回数	5回
<input checked="" type="checkbox"/> ログイン失敗回数	5回
<input checked="" type="checkbox"/> パスワード入力失敗時のリセットまでの時間	60分
<input checked="" type="checkbox"/> ログイン不可状態からの復帰時間	30分

Improvement of the keeping up-to-date environment on your PC
 MyJVN Version Checker

Product Name [ascending]	Version
<input checked="" type="checkbox"/> Adobe Flash Player (ActiveX)	Poor: Older Version
<input checked="" type="checkbox"/> Adobe Flash Player (Plug-in)	---: Not Installed
<input checked="" type="checkbox"/> Java	---: Not Installed
<input checked="" type="checkbox"/> Mozilla Firefox	Poor: Older Version
<input checked="" type="checkbox"/> Mozilla Thunderbird	Good: Latest Version
<input checked="" type="checkbox"/> QuickTime	Good: Latest Version
<input checked="" type="checkbox"/> QuickTime	---: Not Installed

myjvn filtered security information tool

<http://jvndb.jvn.jp/en/apis/myjvn/>

IPA

MYJVN

- To efficiently gather only relevant information from the vast quantity of data stored in JVN iPedia, the vulnerability countermeasure information database.

Filtering Result Window

MyJVN - Filtered Vulnerability Countermeasure Information Tool - Microsoft Internet Explorer

VEND ID Results 1-10 of 32

- JVND-2008-000009 2009.04.08 11:22:26 Apache Tomcat fails to properly handle cookie value
 - Apple Inc.
 - Apple Mac OS X
 - Apple Mac OS X Server
- JVND-2007-000817 2009.02.10 11:32:40 Flash Player vulnerable in handling cross-domain policy files
 - Adobe Systems, Inc.
 - Adobe Flash Player
 - Apple Inc.
- JVND-2008-001043 2008.11.21 12:19:56 X.Org Foundation X server buffer overflow vulnerability
 - Apple Inc.
- JVND-2008-000070 2008.10.22 17:49:26 Internet Explorer vulnerable in handling CDO protocol
 - Microsoft Corporation
 - Microsoft Office XP
- JVND-2008-000016 2008.10.09 13:35:54 Sun Java Runtime Environment (JRE) contains a vulnerability in processing
 - Apple Inc.
 - Sun Microsystems, Inc.
 - JDK
 - JRE
 - SDK

Detailed Information Window

MyJVN - Filtered Vulnerability Countermeasure Information Tool - Microsoft Internet Explorer

Detail of Vulnerability Note

JVND-2008-000009
Apache Tomcat fails to properly handle cookie value

Overview

Apache Tomcat from the Apache Software Foundation contains a vulnerability that could allow a remote attack to a user's web browser. Apache Tomcat from the Apache Software Foundation is a web container that runs Java Servlets and JavaServer Pages. The developer reports that this issue exists because of an incomplete

Affected system

- Apache Software Foundation
 - Apache Tomcat
 - 4.1.0 through 4.1.36
 - 5.5.0 through 5.5.25
 - 6.0.0 through 6.0.14
- Apple Inc.
 - Apple Mac OS X
 - v10.4.11
 - Apple Mac OS X Server
 - v10.4.11
 - v10.5.5
- MIRACLE LINUX CORPORATION
 - MIRACLE LINUX V2.0
 - MIRACLE LINUX V2.1
- Trend Micro, Inc.
 - TrendMicro InterScan Messaging Security Appliance
 - 7.x
 - TrendMicro InterScan Messaging Security Suite
 - 7.x



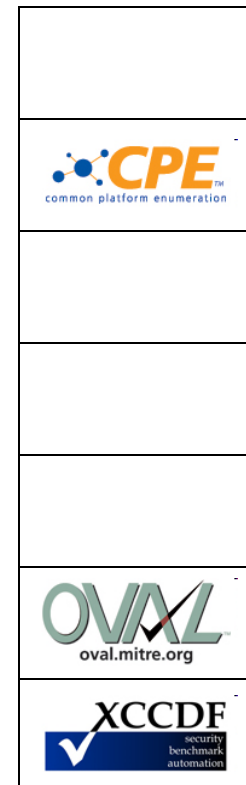
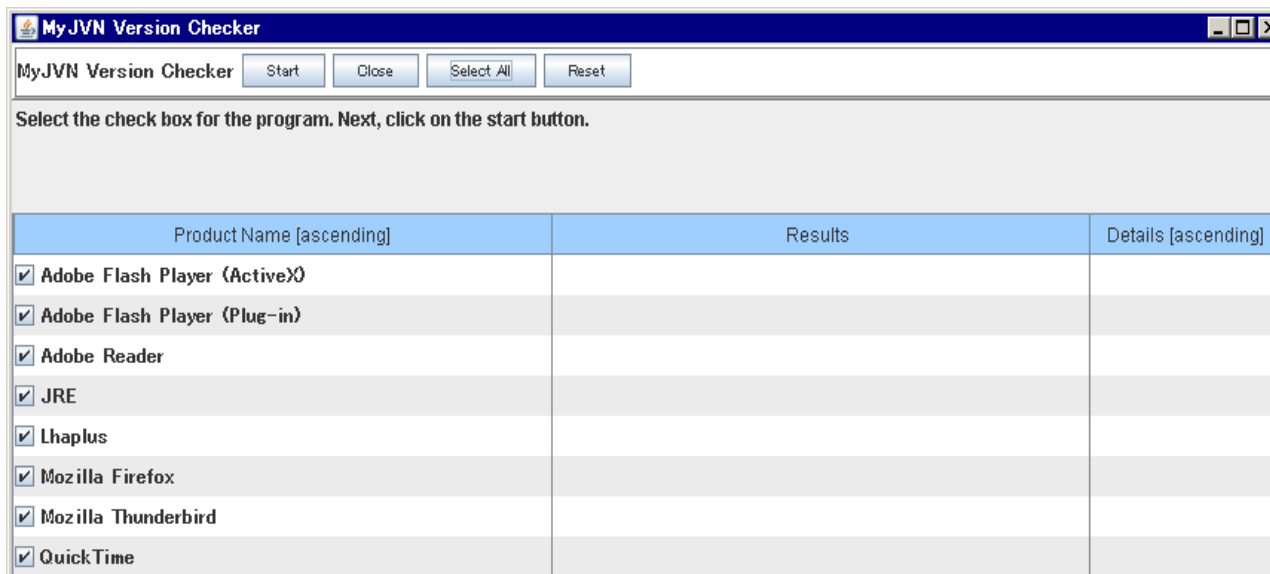
myjvn version checker.

<http://jvndb.jvn.jp/apis/myjvn/vccheck.html>

IPA

MYJ.VN

- 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.



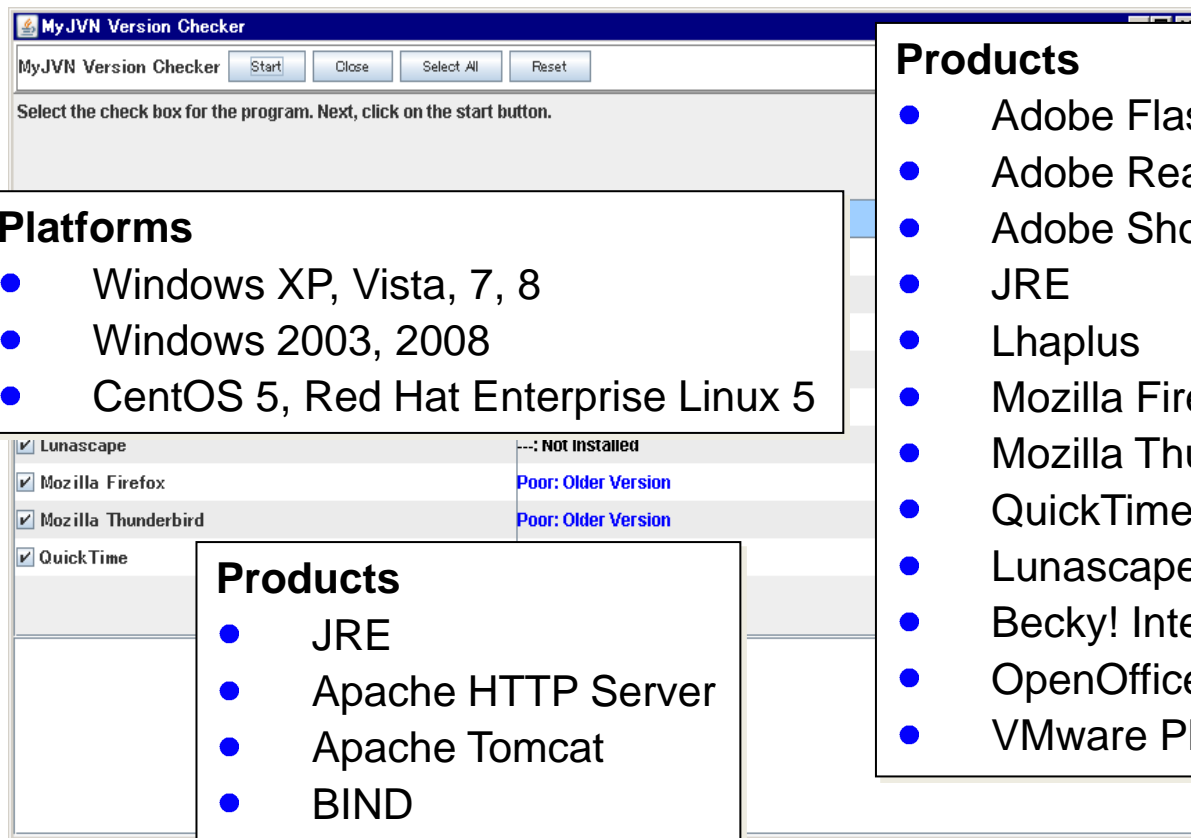
myjvn version checker.

<http://jvndb.jvn.jp/apis/myjvn/vccheck.html>

IPA

myjvn

- MyJVN Version Checker supports multi platforms and multi products.



Platforms

- Windows XP, Vista, 7, 8
- Windows 2003, 2008
- CentOS 5, Red Hat Enterprise Linux 5

Products

- JRE
- Apache HTTP Server
- Apache Tomcat
- BIND
- OpenSSL

Products

- Adobe Flash Player
- Adobe Reader
- Adobe Shockwave Player
- JRE
- Lhaplus
- Mozilla Firefox
- Mozilla Thunderbird
- QuickTime
- Lunascape
- Becky! Internet Mail
- OpenOffice.org
- VMware Player



myjvn security configuration checker. IPA

<http://jvndb.jvn.jp/apis/myjvn/sccheck.html>



- Improvement of the keeping the secure configuration on your PC
 - Splitting the steps into Check and Remedy phase.

MyJVNセキュリティ設定チェッカ

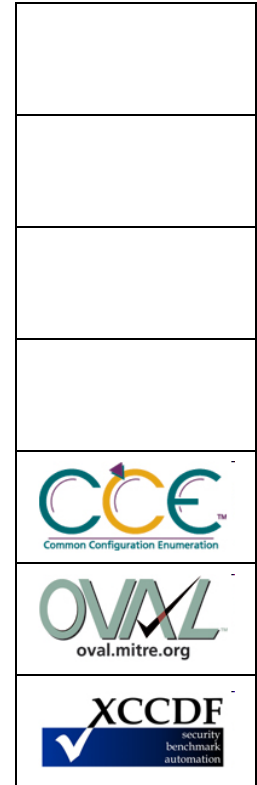
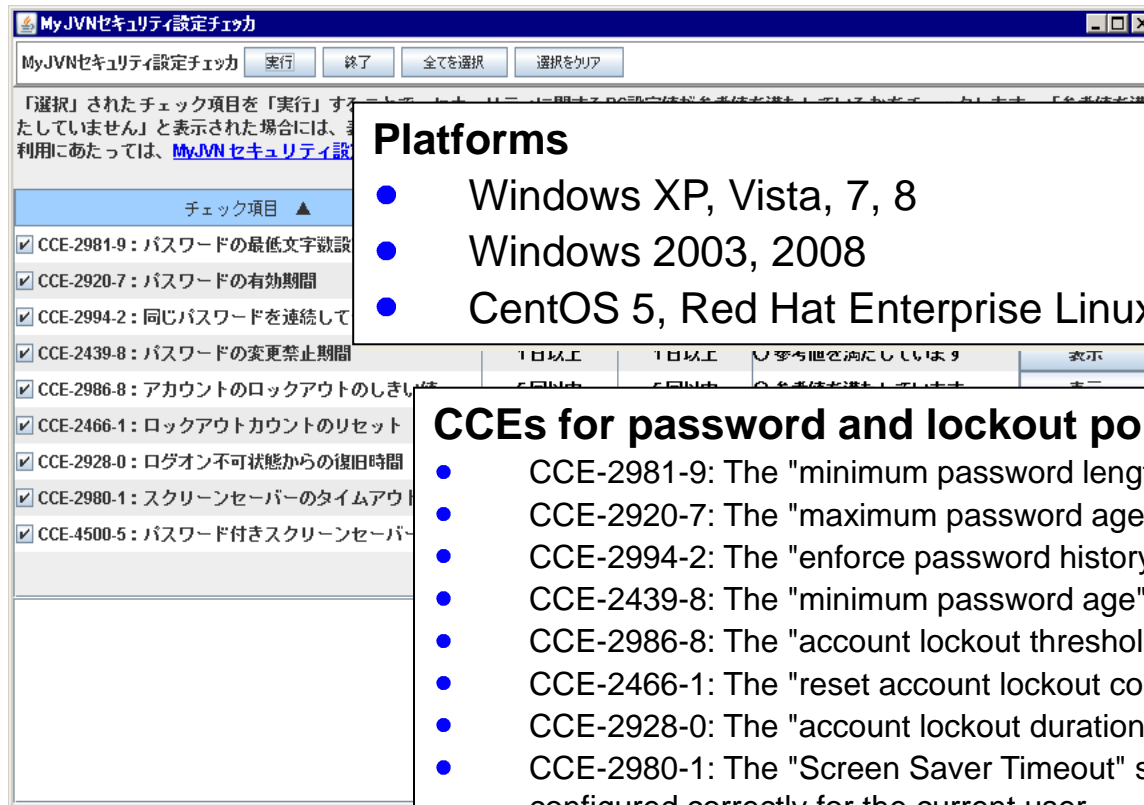
MyJVNセキュリティ設定チェッカ


「選択」されたチェック項目を「実行」することで、セキュリティに関するPC設定値が参考値を満たしているかをチェックします。「参
たしていません」と表示された場合には、表示ボタンを押下後ツール下部の内容を参考にしてPC設定値を変更してください。
利用にあたっては、[MyJVNセキュリティ設定チェッカの使い方](#)も参照ください。

チェック項目 ▲	推奨値	PC設定値	チェック結果 ▲	結果詳
<input checked="" type="checkbox"/> パスワードの最低文字数設定	12文字		CCE-2981-9: Minimum Password Length	
<input checked="" type="checkbox"/> パスワードの有効期間	60日		CCE-2920-7: Maximum Password Age	
<input checked="" type="checkbox"/> 記録するパスワードの履歴数	24個		CCE-2994-2: Enforce Password History	
<input checked="" type="checkbox"/> パスワードの変更禁止期間	1日		CCE-2439-8: Minimum Password Age	
<input checked="" type="checkbox"/> ログオンできなくなるまでのパスワード入力失敗回数	5回		CCE-2986-8: Account Lockout Threshold	
<input checked="" type="checkbox"/> パスワード入力失敗回数のリセットまでの時間	15分		CCE-2466-1: Reset Account Lockout Cou	
<input checked="" type="checkbox"/> ログオン不可状態からの復旧時間	15分		CCE-2928-0: Account Lockout Duration	
<input checked="" type="checkbox"/> パスワード付きスクリーンセーバーの有無	有効		CCE-4500-5: Password protect the screen saver	
<input checked="" type="checkbox"/> USBメモリ自動実行機能の無効化設定	無効		CCE-2154-3: Disable the Autorun functionality	






- MyJVN Security Configuration Checker supports two platforms, the CCEs for password and lockout policies.



 is the framework of machine readable environment with the common enumeration based as a security information sharing and exchanging.

<http://jvndb.jvn.jp/en/apis/>



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

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

- **MyJVN**
<http://jvndb.jvn.jp/en/apis/myjvn/>

- **JVNRSS (JP Vendor Status Notes RSS) Feasibility Study Site**
<http://jvnrss.ise.chuo-u.ac.jp/jtg/>
- **Information Security Early Warning Partnership**
http://www.ipa.go.jp/security/english/quarterlyrep_vuln.html#Partnership

- **JVNRSS (Japan Vulnerability Notes RSS)**
`http://jvndb.jvn.jp/en/schema/jvnrss.html`
`namespace="http://purl.org/rss/1.0/"`
`schemaLocation="http://jvndb.jvn.jp/schema/jvnrss_2.0.xsd"`
- **Qualified Security Advisory Reference (mod_sec)**
`http://jvndb.jvn.jp/en/schema/mod_sec.html`
`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
`http://jvndb.jvn.jp/en/schema/vuldef.html`
`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)