



Summit Days

The Value of

Global Vulnerability Reporting

November 13, 2012

Masato Terada
IT Security Center, IPA

FIRST TC @ KYOTO
Kyoto 2012 FIRST Technical Colloquium
13-15 November 2012



contents.

- **Vulnerability Identifier**
- **vulnerability identification.**
- **# of vulnerabilities.**



vulnerability identifier.

- How many vulnerability identifiers are there in our cyberspace ?

vulnerability identifier.

- How many vulnerability identifiers are there in our cyberspace ?
 - **Database**
 - Regional/national vulnerability databases
NVD, JVN, CNVD etc.
 - Non-government vulnerability databases
Secunia, SecurityFocus, OSVDB, Cisco Security Intelligence Operations, IBM ISS X-Force etc.
 - **Vendor Advisories**
 - Microsoft, Oracle, Cisco, Adobe etc.

vulnerability identifier.

<http://nvd.nist.gov/>


- **NVD (National Vulnerability Database)**

- ID(4 + 4 digits): CVE-2012-1234

- Lang: English

- CVE mapping: one-to-one

- URL: <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1234>



The screenshot shows the NVD website interface. At the top, it is titled "National Vulnerability Database (NVD) National Vulnerability Database (CVE-2012-1234) - Windows Internet Explorer". The page is sponsored by the DHS National Cyber Security Division/US-CERT and NIST. The main heading is "National Vulnerability Database" with the tagline "automating vulnerability management, security measurement, and compliance checking". A navigation menu includes links for Home, SCAP, SCAP Validated Tools, SCAP Events, About, Contact, and Vendor Comments. The main content area is titled "National Cyber-Alert System" and "Vulnerability Summary for CVE-2012-1234". It provides the original release date (02/21/2012), last revised date (02/23/2012), and source (US-CERT/NIST). An "Overview" section describes a SQL injection vulnerability in Advantech/BroadWin WebAccess 7.0, noting that it allows remote authenticated users to execute arbitrary SQL commands via a malformed URL. A note states that this vulnerability exists because of an incomplete fix for CVE-2012-0234.

FIRST TC @ KYOTO

Kyoto 2012 FIRST Technical Colloquium

13-15 November 2012

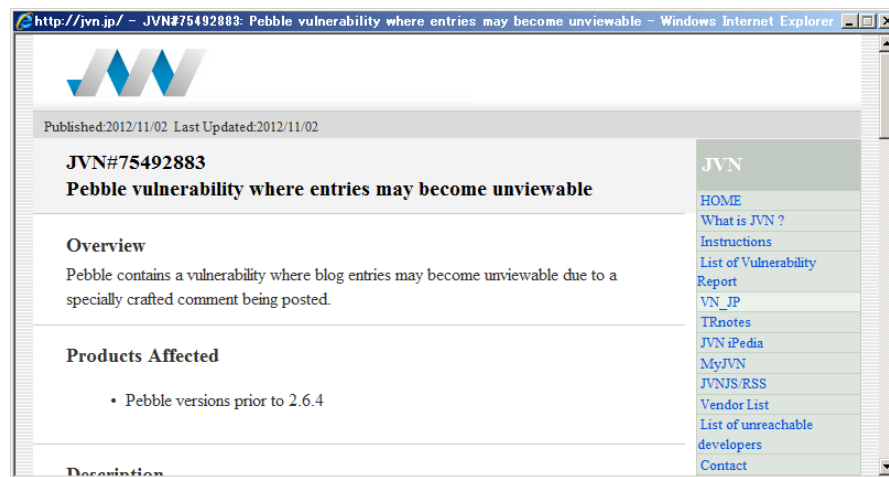


vulnerability identifier.

<http://jvn.jp/>

- **JVN(Japan Vulnerability Database)**

- ID(8 digits): JVN#12345678
- Lang: Japanese/English
- CVE mapping: one-to-one
- URL: <http://jvn.jp/jp/JVN12345678>



FIRST TC @ KYOTO

Kyoto 2012 FIRST Technical Colloquium

13-15 November 2012

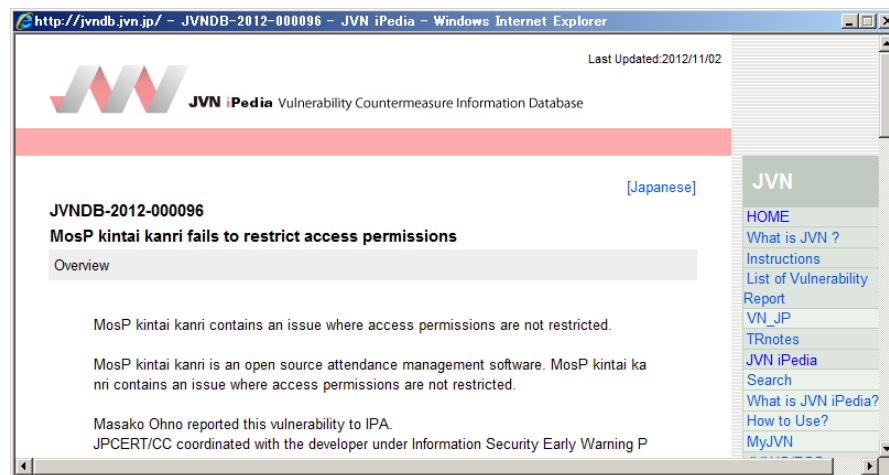


vulnerability identifier.

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

● JVN iPedia

- ID(4 + 6 digits): JVNDB-2012-123456
- Lang: Japanese/English
- CVE mapping: one-to-one
- URL: <http://jvndb.jvn.jp/jvndb/JVNDB-2012-123456>



FIRST TC @ KYOTO

Kyoto 2012 FIRST Technical Colloquium

13-15 November 2012



vulnerability identifier.

<http://www.cnvd.org.cn/>

- **CNVD(China National Vulnerability Database)**

- ID(4 + 5 digits): CNVD-2012-12345
- Lang: Chinese
- CVE mapping: one-to-one
- URL: http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=61059

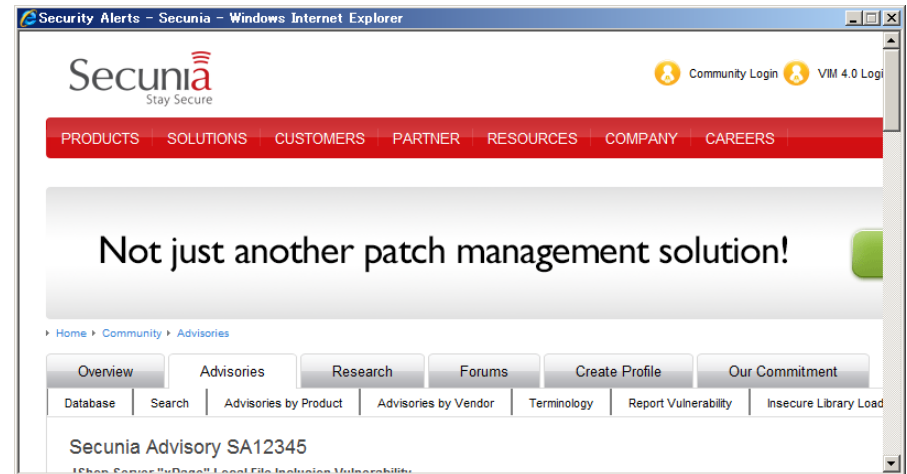


vulnerability identifier.

<http://secunia.com/>

● **Secunia**

- ID(5 digits): SA12345
- Lang: English
- CVE mapping: one-to-many
- URL: <http://secunia.com/advisories/12345>

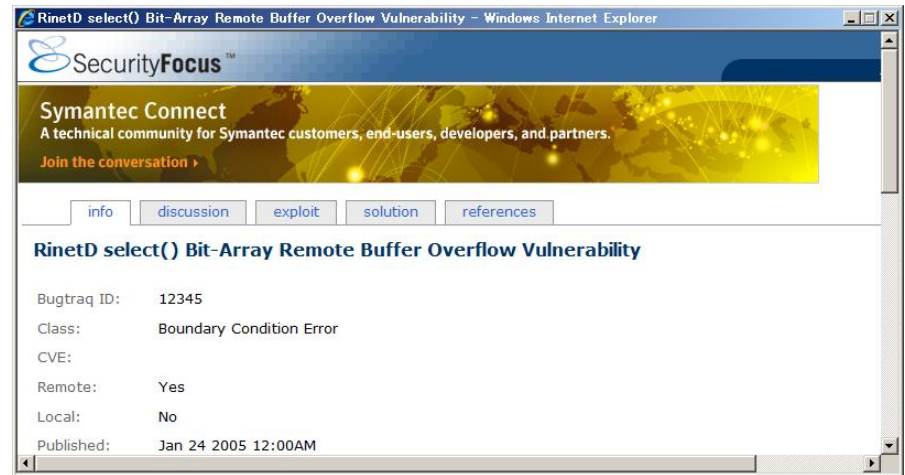


vulnerability identifier.

<http://www.securityfocus.com/>

● SecurityFocus

- ID(variable digits): 12345 (aka. bid12345)
- Lang: English ^^^^^ current longest id is 5 digits
- CVE mapping: one-to-many
- URL: <http://www.securityfocus.com/bid/12345>

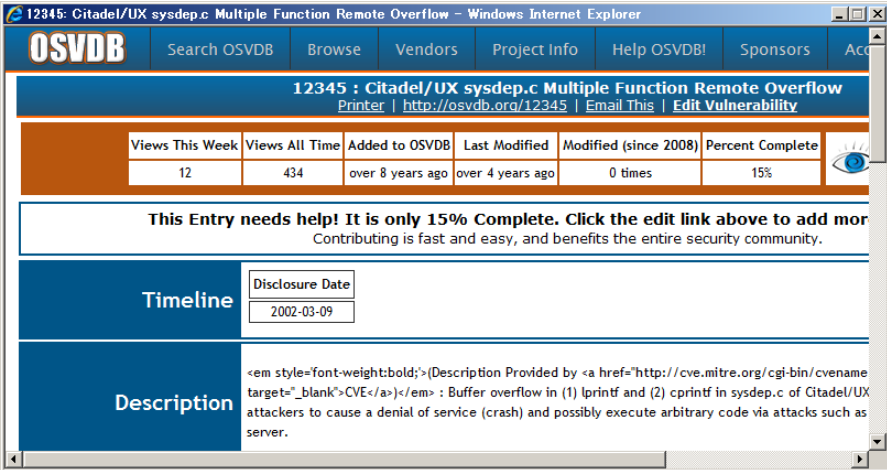


vulnerability identifier.

<http://osvdb.org/>

- **OSVDB (The Open Source Vulnerability Database)**

- ID(variable digits): 12345
- Lang: English ^^^^ current longest id is 5 digits
- CVE mapping: one-to-many
- URL: <http://osvdb.org/show/osvdb/12345>



The screenshot shows a web browser window displaying the OSVDB entry for ID 12345. The page title is "12345 : Citadel/UX sysdep.c Multiple Function Remote Overflow". The navigation bar includes "OSVDB", "Search OSVDB", "Browse", "Vendors", "Project Info", "Help OSVDB!", "Sponsors", and "Acc". Below the title, there are links for "Printer", "http://osvdb.org/12345", "Email This", and "Edit Vulnerability". A table provides statistics: Views This Week (12), Views All Time (434), Added to OSVDB (over 8 years ago), Last Modified (over 4 years ago), Modified (since 2008) (0 times), and Percent Complete (15%). A message states: "This Entry needs help! It is only 15% Complete. Click the edit link above to add more. Contributing is fast and easy, and benefits the entire security community." The "Timeline" section shows a "Disclosure Date" of "2002-03-09". The "Description" section contains a bolded text: "(Description Provided by : Buffer overflow in (1) lprintf and (2) cprintf in sysdep.c of Citadel/UX attackers to cause a denial of service (crash) and possibly execute arbitrary code via attacks such as server.)".

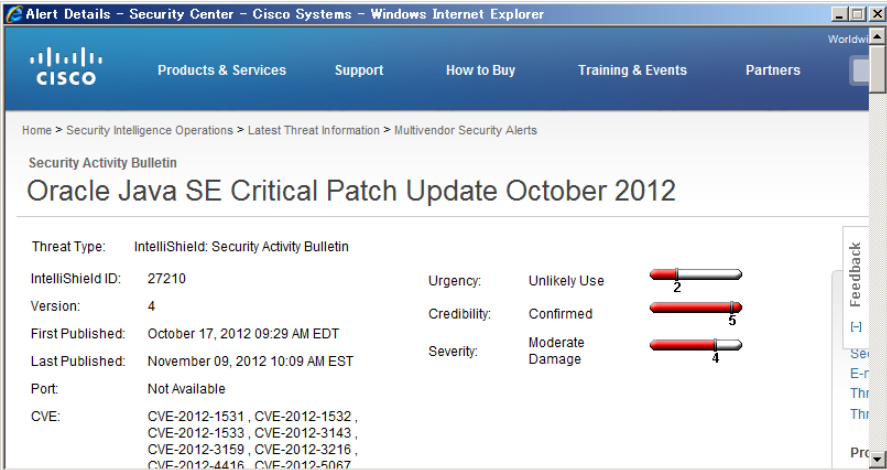


vulnerability identifier.

<http://tools.cisco.com/security/center/>

● Cisco Security Intelligence Operations

- ID(5 digits): 12345
- Lang: English
- CVE mapping: one-to-many
- URL: <http://tools.cisco.com/security/center/viewAlert.x?alertId=12345>



The screenshot shows the 'Alert Details' page in the Cisco Security Center. The page title is 'Alert Details - Security Center - Cisco Systems - Windows Internet Explorer'. The breadcrumb trail is 'Home > Security Intelligence Operations > Latest Threat Information > Multivendor Security Alerts'. The main heading is 'Security Activity Bulletin' followed by 'Oracle Java SE Critical Patch Update October 2012'. The alert details are as follows:

Threat Type:	IntelliShield: Security Activity Bulletin	Urgency:	Unlikely Use	2
IntelliShield ID:	27210	Credibility:	Confirmed	5
Version:	4	Severity:	Moderate Damage	4
First Published:	October 17, 2012 09:29 AM EDT			
Last Published:	November 09, 2012 10:09 AM EST			
Port:	Not Available			
CVE:	CVE-2012-1531, CVE-2012-1532, CVE-2012-1533, CVE-2012-3143, CVE-2012-3159, CVE-2012-3216, CVE-2012-4416, CVE-2012-5067			

FIRST TC @ KYOTO

Kyoto 2012 FIRST Technical Colloquium

13-15 November 2012

12



vulnerability identifier.

<http://xforce.iss.net/>

● IBM ISS X-Force

- ID(short subject + variable digits): speak-freely-udp-bo (12345) <<<<< current longest id is 5 digits
- Lang: English
- CVE mapping: one-to-many
- URL: <http://xforce.iss.net/xforce/xfdb/12345>



vulnerability identification.

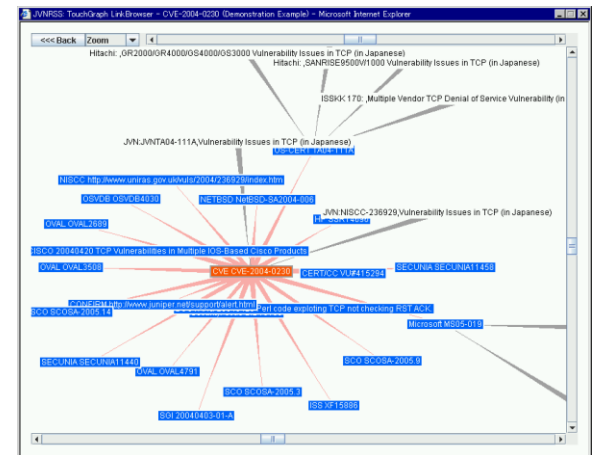
- How do we make a relationship of vulnerability information ?



vulnerability identification.

- How do we make a relationship of vulnerability information ?
- Currently, we can use Common Vulnerabilities and Exposures (CVE), which is the most well known vulnerability identification scheme.

CVE is best and unique reference ID in world wide.



of vulnerabilities.

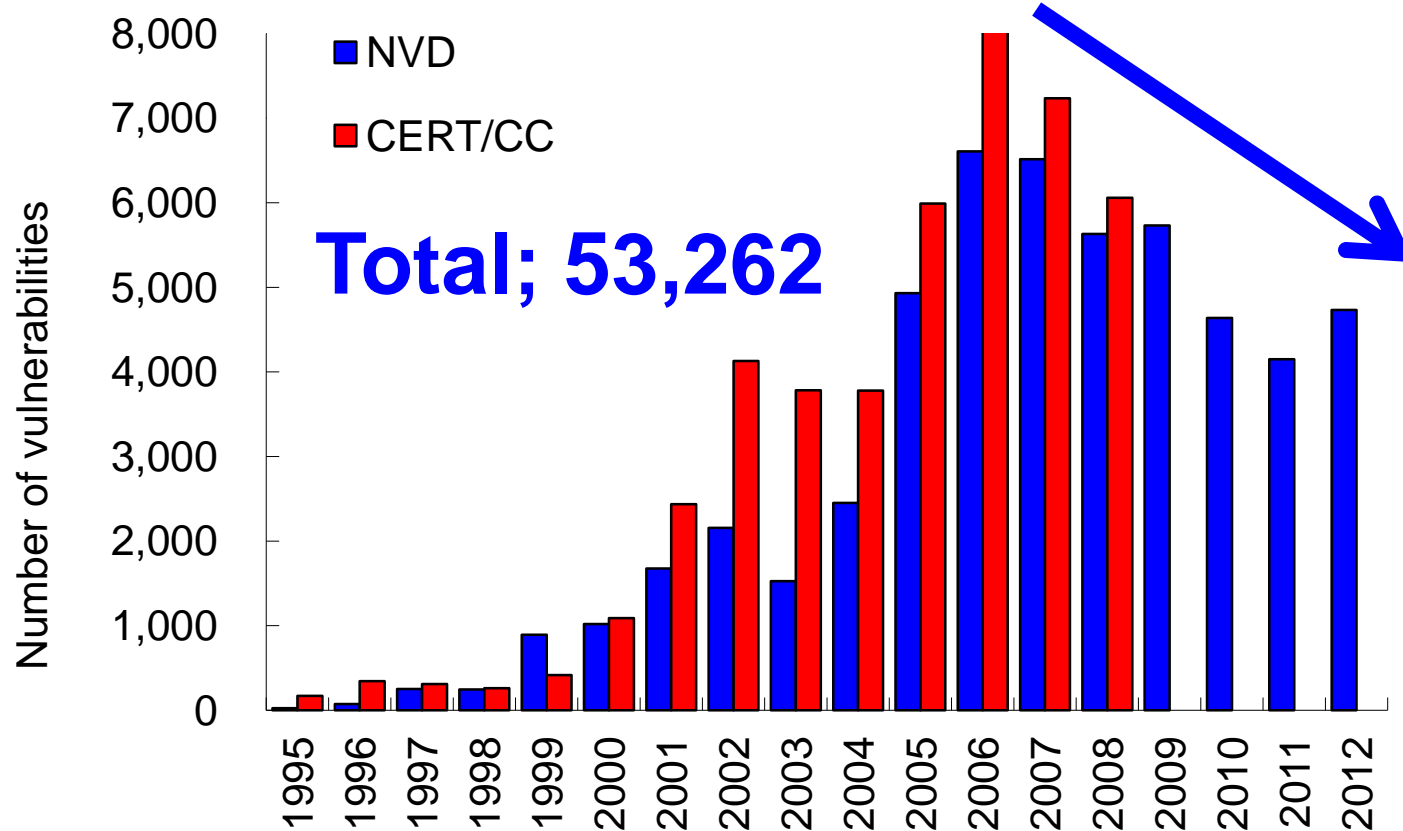
- How many # of vulnerabilities ?



of vulnerabilities.

<http://nvd.nist.gov/>

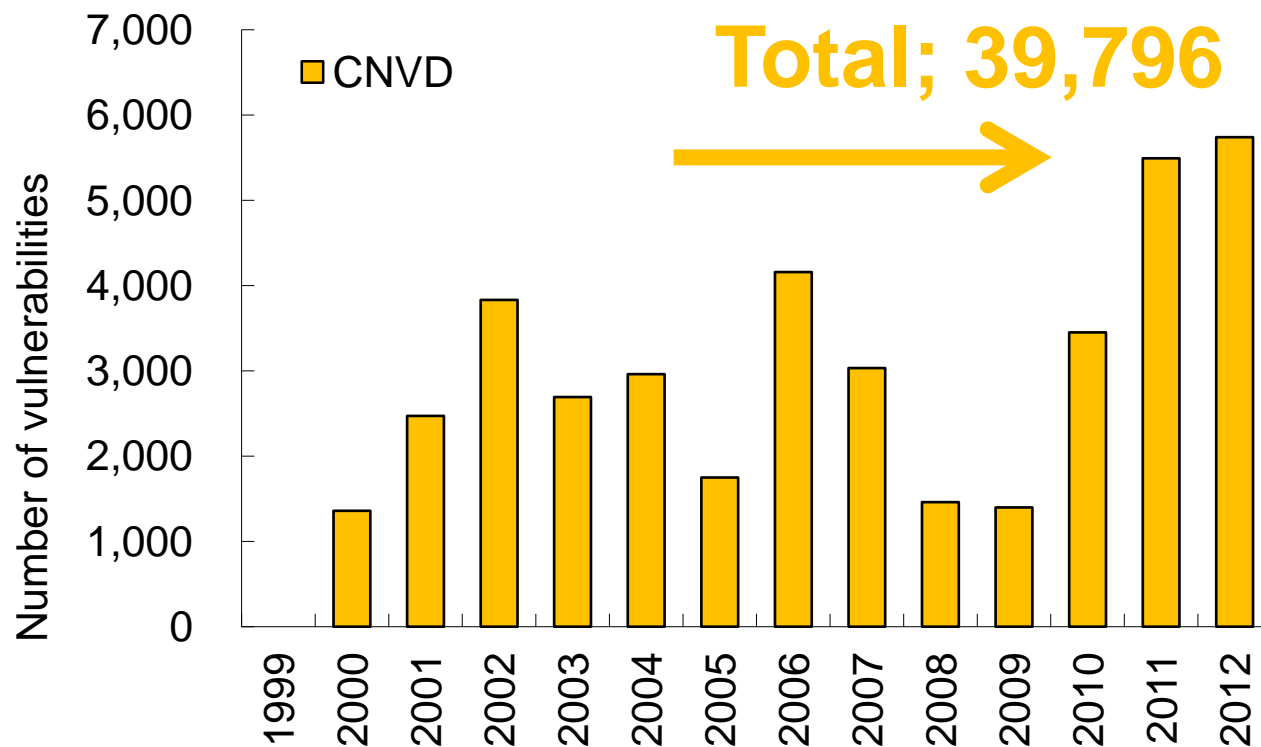
● NVD (National Vulnerability Database)



of vulnerabilities.

<http://www.cnvd.org.cn/>

- **CNVD(China National Vulnerability Database)**



of vulnerabilities.

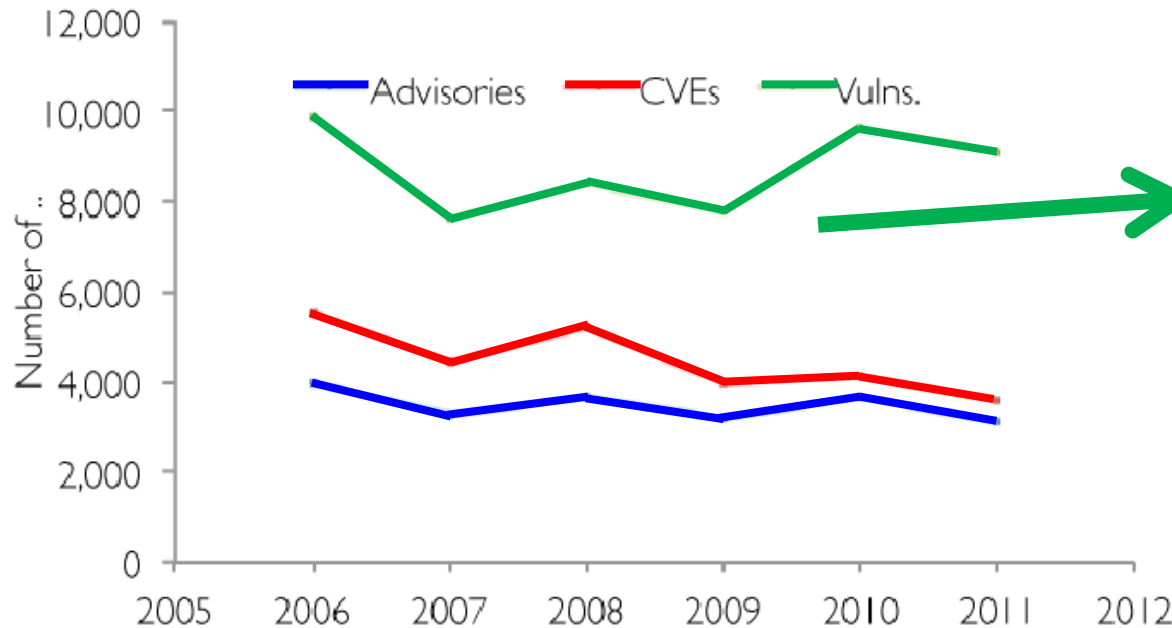
<http://secunia.com/>

- **Secunia**

Average 2006-10; 8,663

Total 2011; 9,132

Global Vulnerabilities History
all products of all vendors



**Global Vulnerability
Reporting will provide best
solution of this questions.**

