Global Vulnerability Reporting (GVR): Perspectives from CVE

November 13, 2012

Steve Christey, coley@mitre.org

David Mann, damann@mitre.org

MITRE

DISTRIBUTION IS LIMITED TO ORGANIZATIONS IN FIRST Cyber-Security Knowledge Structuring Group

DISCLAIMER

- **These slides were prepared to facilitate discussion about Global Vulnerability Reporting in the FIRST Technical Colloquium in Kyoto, Japan, November 13 to 15.**
- **The opinions and recommendations in these slides do not necessarily represent an official position of The MITRE Corporation.**
- **The opinions and recommendations in these slides are subject to change without notice.**

THIS SLIDE PRESENTATION SHOULD NOT BE PUBLISHED. DISTRIBUTION IS LIMITED TO FIRST MEMBERS FOR THE PURPOSE OF FORMING A GLOBAL VULNERABILITY REPORTING SIG.

Arigatou gozaimasu

(Thank you)

JPCERT/CC, IPA, and FIRST Japan

Outline

- State of CVE
- Evolution of CVE content decisions
- CVE ID management
- Other GVR considerations

SECTION 1 – STATE OF CVE

Vulnerability Information: An Inconvenient Truth

Fast

Cheap

Good

… pick any two

CVE is Growing… but not Globally

- **MITRE is publishing more CVEs**
  - **Process and infrastructure improvements**
  - **More analysts**
  - **More CVEs from Candidate Numbering Authorities (CNAs)**
- **We will change the CVE ID syntax so there can be more than 10,000 IDs in a single year**
  - **Subject to Editorial Board review**
  - **MAYBE "CVE-2014-012345" but not sure**
- **We are defining CVE's scope more clearly**
  - **Focus on the English-language software market**
  - **Products / sources CVE will cover**

- ***CVE cannot solve the Global Vulnerability Reporting problem itself***

CVE Sources and Products Details

Full-Coverage Sources

- Adobe
- Apache Software Foundation: Apache HTTP Server
- Apple
- Attachmate: Novell
- Attachmate: SUSE
- Blue Coat - kb.bluecoat.com
- CA - support.ca.com
- Check Point: Security Gateways product line (supportcenter.checkpoint.com)
- Cisco: Security Advisories/Responses
- Citrix - support.citrix.com
- Debian
- Dell Desktop/Notebook product lines
- Dell SonicWALL Network Security product line - Service Bulletins
- EMC, as published through Bugtraq
- F5 - support.f5.com
- Fortinet FortiGate product line (kb.fortinet.com)
- Fujitsu Desktop/Notebook product lines
- Google: Google Chrome (includes WebKit)
- HP: Security Bulletins
- IBM: issues in IBM ISS X-Force Database
- Internet Systems Consortium (ISC)
- Juniper: juniper.net/customers/support (JunOS?)
- Lenovo Desktop/Notebook product lines
- McAfee - kc.mcafee.com
- Microsoft: Security Bulletins/Advisories
- MIT Kerberos
- Mozilla
- OpenSSH
- OpenSSL
- Oracle: Critical Patch Updates
- RealNetworks (real.com)
- Red Hat
- RIM/BlackBerry- blackberry.com/btsc
- Samba Security Updates and Information
- SAP - scn.sap.com/docs/DOC-8218
- Sendmail
- Sophos - sophos.com/support/knowledgebase
- Symantec: Security Advisories
- Ubuntu (Linux)
- VMware
- Websense - websense.com/content/support.aspx
- HP: TippingPoint DVLabs
- HP: TippingPoint Zero Day Initiative
- ICS-CERT: ADVISORY
- MITRE CNA open-source requests
- US-CERT: Technical Cyber Security Alerts
- VeriSign iDefense

Partial-Coverage Sources

- Android (associated with Google or Open Handset Alliance)
- Apache Software Foundation: Apache Tomcat
- Apache Software Foundation: other
- CentOS
- Check Point: checkpoint.com/defense/advisories/public/summary.html
- Cisco: Release Note Enclosures (RNE)
- Drupal
- Fedora
- FoxIt Support Center - Security Advisories
- FreeBSD
- Gentoo (Linux)
- Google: other (not Chrome or Android)
- IBM ISS X-Force for non-IBM products
- IBM: issues not in IBM ISS X-Force Database
- Joomla!
- Juniper - JTAC Technical Bulletins
- kernel.org
- Mandriva
- NetBSD
- OpenBSD
- PHP core language interpreter
- SCO
- TYPO3
- WordPress
- attrition.org/pipermail/vim
- AusCERT
- Core Security CoreLabs
- DOE JC3 (formerly DOE CIRC and CIAC)
- Full Disclosure
- HP: TippingPoint Pwn2Own
- http://www.exploit-db.com/
- ICS-CERT: ALERT
- Juniper: J-Security Center - Threats and Vulnerabilities
- Microsoft: Vulnerability Research (MSVR)
- oss-security
- OSVDB
- Packet Storm
- Rapid7 Metasploit
- Secunia
- SecuriTeam
- SecurityTracker
- Symantec: SecurityFocus BugTraq (securityfocus.com/archive/1)
- Symantec: SecurityFocus Bugtraq ID (securityfocus.com/bid)
- United Kingdom CPNI (formerly NISCC)
- US-CERT: Vulnerability Notes

Must-Have Products

- Adobe: all
- Apache Software Foundation: All
- Apple: all
- Attachmate: Novell
- Attachmate: SUSE
- Blue Coat: all
- CA: all
- Check Point: Security Gateways product line
- Cisco: all
- Citrix - support.citrix.com
- Debian: all
- Dell: Desktop/Notebook product lines
- Dell: SonicWALL Network Security product line
- EMC: all
- F5: all
- Fortinet: FortiGate product line
- Fujitsu: Desktop/Notebook product lines
- Google: Google Chrome (includes WebKit)
- HP: all
- IBM: all
- Internet Systems Consortium (ISC): Bind
- Juniper: all
- kernel.org (Linux kernal)
- Lenovo: Desktop/Notebook product lines
- McAfee: all
- Microsoft: all
- MIT Kerberos: all
- Mozilla: all
- MySQL: all
- OpenLDAP: all
- OpenSSH: all
- OpenSSL: all
- Oracle:all
- PHP: core language interpreter
- RealNetworks:all
- Red Hat: all
- RIM/BlackBerry: all
- Samba: all
- SAP: all
- Sendmail: all
- Sophos: all
- Symantec: all
- Ubuntu: all
- VMware: all
- Websense: all

Quantity and Quality Issues in Vulnerability Disclosures

- More vulnerability researchers (while others stop disclosing)
- Better discovery and exploit methods
- More known vulnerability types
- More vulnerabilities per disclosure
  - Often 2 to 5 CVEs covering 3 to 30 bugs, sometimes 50+ CVEs
- Wider gaps in advisory quality
- More complex vulnerabilities
- More analytical complexity and effort

Why was there a Decline in CVE/NVD? One Reason: More Complex Vulnerabilities

- CVE-2012-4564: missing return value check → improperly handled integer-overflow warning → memory allocation of 0 bytes → heap-based buffer overflow
  - (CWE-252 -> CWE-190 -> [no CWE] -> CWE-122)
- CVE-2012-4487: "parent" user can switch to "child" user without having the allowed privilege
  - Must understand business logic to identify (and describe) as a vulnerability
- CVE-2012-3511: race condition leads to use-after-free
- CVE-2012-1103: special tags in a specific file format allow "injection" in email client that enables sending arbitrary files to attacker
- CVE-2012-3420: negative return value is treated as an error even when it wasn't, leading to memory leak
- CVE-2012-4513: unexpected sign extension → heap-based buffer over-read
- Root-cause CSRF often enables other resultant vulns (SQL injection, XSS, code injection, ...

CVE is Community-Guided

- MITRE is a not-for-profit organization
  - CVE is funded by US-CERT (Dept. of Homeland Security)
- MITRE formed the CVE Editorial Board to seek consensus and guidance
  - http://cve.mitre.org/community/board/index.html
  - Recently: source/products lists, CVE ID syntax, GVR
- Early Board discussions and voting on entries (since abandoned) led to formulation of "Content Decisions"
- CVE's Content Decisions are editorial policies
  - Inclusion – when to assign an ID
  - Counting/abstraction – how many IDs to assign
- Content Decisions are the most difficult and most important challenge for new CVE analysts and CNAs
- Candidate Numbering Authorities (CNAs) decentralize the assignment of CVE identifiers

CVE Content Creation and CNA Relationships

- Proper CVE counting takes non-zero time and training
- CNA coordination is a hidden cost that does not directly influence the number of CVEs published
- Many vendors do not publish enough vulnerabilities to become a CNA
- CNA relationships help considerably, but:
  - This is voluntary (relatively small cost)
  - MITRE still does post-disclosure CVE entry creation/maintenance
  - CNAs may be unwilling to incur costs of populating and maintaining CVE content
  - CNAs do not always follow the CVE content decisions as intended

SECTION 2 – THE EVOLUTION OF CVE CONTENT DECISIONS

Inclusion ("What Gets an ID")

- Day 1 (1999): "all publicly known vulnerabilities"
  - Now: too many to cover
  - Now: are bug trackers or customer-only advisories "public"?
  - Now: historical vulnerabilities are covered by OSVDB
    - OSVDB:79400 - Marconi Wireless Telegraph (1903)
- Then: we thought we could define "vulnerability" properly
  - But what's OK for one is bad for another
  - Now: need to know intended security policy / business logic
- Then: we shouldn't cover configuration, IDS, malware
  - Now: CCE, CEE, CME/MAEC – but still some overlap with CCE
- Then: if it was reported on Bugtraq, it was probably real
  - Now: anything goes, many false positives
  - Now: security impact not always established
  - Now: external CNAs sometimes assign CVEs when CVSS = 0.0

Inclusion (Continued)

- Then: "we don't cover live web sites"
  - Now: no change, we just call it "cloud" and "services"
  - A major gap for tracking / trend analysis
- Then: "we don't cover SCADA / ICS" (2002?)
  - Now: ICS-CERT is a CNA
  - Now: coffee makers, medical devices cause physical damage

More researcher interest

- Then: "we don't cover cell phones" (2003?)
  - Now: we cover phone OS, jailbreaks, and 3rd party apps
- Then: Limited types of information leak "exposures" (e.g., full path disclosure)
  - Now: if the leak is a private memory address (important for ASLR bypass), then according to Linux it's an "exposure" to remove, but in Windows it's an intentional "feature"

Abstraction/Counting ("How Many IDs to Assign")

- Day 1 (1999): "one CVE per vulnerability"
  - Didn't work - not enough information, high analysis cost, too many IDs for some consumers
- Next: "one CVE per bug type, per version"
  - Example: separate IDs for XSS, buffer overflows, SQL injection
  - Covers most situations, even today
  - Differing opinions about closely-related bug types
  - Sometimes an analyst must knowingly combine multiple distinct bugs into one ID
- Next: defining how to manage overlapping disclosures
  - Disclosure 1: bugs A, B, C, and D in version 1.0
  - Disclosure 2: bugs C, D, E, and F in version 2.0
- Next: "Separate root cause from bug type, if known"
  - "Classic" buffer overflows vs. integer overflows

Abstraction/Counting (Continued)

- Now: decision tree with about 20 questions (not public)
- Now: “one CVE per bug type, per version, per researcher, per 1-day disclosure period for that researcher” (MITRE)
- Now: researchers can chain 10 bugs together for reliable remote code execution without authentication
- Now: “one CVE per bug ID, unless a Linux distribution says they can fix one bug but not the other, and re-evaluate when new bugs are found while fixing the original bug” (oss-security mailing list)
- Now: “only a couple CVEs for this fuzzer with 1,000,000 tests where different tests affect different implementations with different codebases”
- Now: software vendor CNAs sometimes use their own method of counting

CVE Content Decisions – Lessons Learned

- Software development changes over time
- Disclosure practices change over time
- Vulnerability details change over time
- Researcher expertise changes over time
- CVE's own expertise changes over time

(… and varies by region, country, vendor, or individual)

- Perfect rules and consistency are not possible
  - CNAs will not / cannot always follow guidelines
- You won't always get it right… but when you realize it, it can be too late
  - Too many people are already using the ID
  - Only SPLIT or MERGE post-disclosure in extreme situations
- Sometimes have to allow CD violations if it's best for users
  - Example: CVE-2012-0217 is a class of implementation problems for Intel chips where each OS should have received its own CVE

Other CVE Lessons Learned

- There cannot be a perfect coordination ID scheme
- We made the right choice with a simple ID that did not encode taxonomy or semantics
  - Even the year isn't ideal
- Getting the ID in the first public disclosure ensures that it is used everywhere
  - Otherwise, not everybody updates their mappings
  - But, early disclosure can mean imperfect abstraction
- The CVE ID should not be used as the primary ID for any other scheme
  - This rule should probably apply to any coordination ID

SECTION 3 – CVE ID MANAGEMENT

CVE ID Life Cycle

- Candidate Numbering Authority (CNA) reserves an ID pool
  - These IDs have a default description "** RESERVED **"
- CNAs assign a CVE ID to a specific issue(s)
- MITRE CNA privately reserves/assigns a CVE ID for non-CNAs
- If a CVE ID is assigned before disclosure
  - Advisory is published with reserved CVE
  - MITRE notices advisory
  - MITRE detects that a reserved ID is being used
  - MITRE changes description/references of the reserved CVE
- If a public disclosure has no CVE ID
  - MITRE is primary assigner (Red Hat handles oss-security)
  - MITRE notices advisory
  - MITRE reserves/assigns new CVE

Duplicate CVE ID Management

- http://cve.mitre.org/cve/editorial_policies/duplicates.html
- **Duplicates happen when disclosure is not coordinated, or when CVE assignment is not coordinated**
- **The rate of CVE duplicates is around 0.5%**
  - **… but it FEELS much worse and is technically painful**
- **One CVE is kept, the other is REJECTed in description**
  - **Always leave a forward pointer to the correct ID**
- **Many complicated scenarios**
  - **One CVE has a description and one shows as "RESERVED"**
  - **When two CNAs publish separate IDs for the same issue**
    - **… especially in 0-day situations?**
  - **CVE number typos in advisories**
  - **What if multiple IDs are published for an issue from different products with the same shared code?**

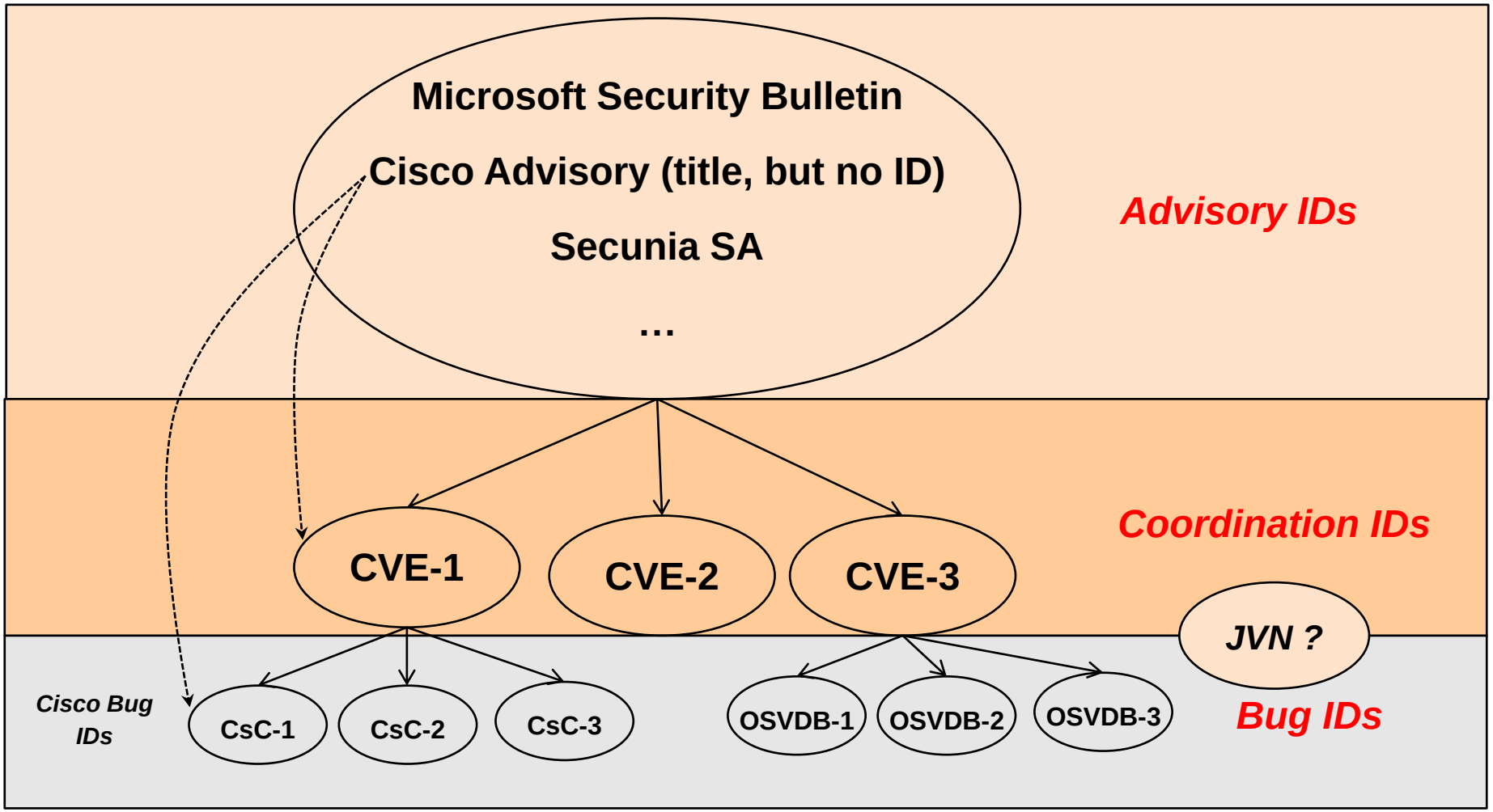
Multiple Types of "Vulnerability" IDs: The ABCs

- **A**dvisory ID
  - MS12-067 (Microsoft), SA12345 (Secunia), …
  - No ID: Oracle, Cisco, …
  - HP (multiple IDs)
- **B**ug ID (often "Vulnerability")
  - CERT-VU, JVN, Cisco Bug ID, OSVDB, …
  - Rarely used by researchers

(counting is only from publisher's perspective)

- **C**oordination ID *(counting must be usable by multiple perspectives)*
  - CVE-xxxx-yyy
- Many things have more than one ID
  - cars, computers, books, humans, …
- Each ID type serves different purposes and audiences
- One ID type can be used (poorly) for a different type of thing

Different Usage or Audience = Different IDs, Different Levels of Abstraction



CVE Abstraction ("Counting") Versus Other Approaches

- CVE's level of abstraction has evolved to be IN THE MIDDLE
  - The right place for a coordination ID
  - Most usable by the most people
- The content decisions rely on information that is usually stable, and often published early
- Challenges
  - Difficult to "count" correctly and consistently
  - Difficult to SPLIT or MERGE after initial publication
  - Abstraction choices are not always obvious or "natural;" they seek consistency across ALL vulnerabilities and disclosures, regardless of how much detail is available for an individual vulnerability
  - Abstraction choices are still affected by what information is available at the time of assignment – and that information can change

Primary ID for Each Market

- **CVE encourages the distinction between:**
  - **Proprietary IDs associated with disclosures**
    - **i.e., advisory or bug IDs**
  - **Coordination IDs (like CVE) that can be used to cross-reference multiple disclosures from different sources**

- **CVE encourages identification & recognition of cross-reference (coordination) IDs within each GVR market**
  - **In markets where there are multiple disclosers (as is the case in the English-based market), CVE encourages the development of a coordination ID (similar to CVE)**
  - **In markets where disclosures are more centrally controlled, the coordination ID could be the ID scheme of that discloser**

Single ID for GVR?

- CVE encourages a “go-slow” approach regarding any discussions of an ID scheme to be used for GVR
- Not yet clear:
  - which markets will be participating
  - if markets can define reasonable boundaries
  - how disclosure will work in various markets
  - if each market will have an organization that issues primary IDs
  - a primary ID issuing organization will appear in each market
  - how much coordination will be required among primary ID issuers

SECTION 4 – OTHER GVR CONSIDERATIONS

GVR Needs to be International

- **GVR can only be addressed adequately in a forum in which:**
  - **Members have direct experience with vulnerability reporting, coordination, and response**
  - **There is real international representation**

- **CVE believes that FIRST is the most promising venue for productive GVR discussions**

Disclosure Issues (in the English-based Market)

- In 2000 and earlier, vendors did not always fix vulnerabilities, which forced researchers to disclose without coordination
- Best coverage demands tracking both vendor and independent sources
  - No US regulations on software vendors requiring disclosure
    - Vendors almost never provide 100% coverage (due to low severity, unsupported products, lack of awareness)
  - No US law stopping independent disclosure (but laws or legal threats have had a chilling effect in multiple countries)
- No well established norms for vulnerability details
  - CVE entry creation relies heavily on human analysis and often integrates details from multiple disclosures
  - Vendor details vary widely
- Proprietary IDs for initial disclosure simplify data gathering and tracking

Reporting Trends: Volume Increasing?

- The global software base is growing fast
  - More lines of code
  - More software packages
  - More code sharing
  - More complex interactions between packages
- Vulnerability research quality/quantity is changing

Reporting Trends: Could Volume Decrease?

- **Incentives for reporting are decreasing or shifting**
  - **Some vendors are providing less information**
  - **Government laws have had a noticeable effect**
  - **White, gray, and black market value for vulnerabilities suppresses or delays public disclosures**
  - **Auto-updates / silent updates**
  - **Vulnerabilities more difficult to find in solid software**
- **Will GVR be overwhelmed, go silent, or become tightly regulated?**
- **Will there be a fundamental shift from vulnerability tracking to patching? (but there are always 0-days)**

Different Markets/Different Disclosures?

- CVE is a result of how disclosures happen in the English-based software market
  - Well established cultural attitudes favoring disclosure
  - No regulatory requirements on vendors to disclose
  - Mature software vendors typically disclose vulnerabilities to meet customer demand
  - Independent researchers often publish without coordination
- Disclosure practices may evolve differently in different markets
  - Different countries may impose different requirements on vendors relative to disclosure
  - Markets may have different cultural attitudes relative to access to vulnerability information
  - Vendors may respond to customer requests differently
  - Different customer demands for access to details

Unclear Evolution of Global Codebase

- **Globalization affects amount of shared code around the globe**
  - **This affects the degree of coordination that will be needed among the different markets**
  - **Many English-based products use a shared codebase that is localized for non-English markets**
  - **There are increasing numbers of software products that are only present in their native language markets**
    - **Vulnerabilities generally won't imply vulnerabilities in another market**

Coordination and the Language Barrier

- **JP-CERT is a CVE Candidate Numbering Authority (CNA):**
  - **JP-CERT has made extraordinary effort (for which we are grateful)**
  - **JP-CERT has been willing to work in English**
  - **MITRE cannot easily analyze reports written in Japanese**
- **Coordination across market/language boundaries will require language considerations similar to those seen in:**
  - **International business**
  - **Law enforcement**
- **More markets, more languages**

Recognition of Multiple Language-based Markets

- CVE encourages recognizing and understanding multiple GVR markets
  - Native language is a central issue
  - National regulatory differences are another issue
- CVE encourages definition of these markets in terms of
  - Public, Internet-accessible sources of vulnerability information
  - (Most important) Vendors and products within that market
- CVE has begun this process already

Better Disclosures → Better Coordination, Better Coordination → Better Disclosures

- CVE encourages disclosers to use locally controlled (i.e. proprietary) IDs
  - Makes their repository of disclosures easier to reference
- CVE encourages disclosers to use cross-referencing (coordination) IDs that count vulnerabilities in similar ways
  - http://cve.mitre.org/cve/editorial_policies/cd_overview.html
- CVE encourages disclosers to publish their information in standardized formats and structures such as CVRF
  - http://www.icasi.org/cvrf
- CVE encourages disclosers to follow disclosure best practices – responsible/coordinated disclosure
  - Coordination produces higher-quality information
  - http://www.dhs.gov/xlibrary/assets/vdwgreport.pdf
  - http://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00

QUESTIONS AND DISCUSSION

BACKUP SLIDES

Scope Issues

- Original goal was “all publicly disclosed vulnerabilities”
- Expansion of global software market has forced more concrete definition of scope
  - Full-coverage sources: Nearly all issues will get a CVE ID (assuming they should be included), regardless of the criticality.
  - Partial Coverage Sources: The source will be actively monitored but issues will be associated with CVE entries based on a variety of editorial judgments (e.g. criticality).
  - Must-have products: Will issue a CVE ID provided that:
    - a) The disclosure is published in at least one source that is listed as either "full coverage" or "partial coverage“
    - a) The disclosure is publicly associated with the product with a reasonably recognizable variant of the product name
- MITRE CVE is now in position to define its scope within the larger GVR context
  - Full lists available on request

Vulnerability Advisory Publication and Practices (VAPP)

- Informal side project by Steve Christey (MITRE), Carsten Eiram (Secunia), Brian Martin (OSVDB)
  - Not public, but we can be convinced to finish it ;-)
- What are the current practices? Vendors, researchers, coordinators
- What seems to work best for vulnerability databases (and their consumers)?
- Includes process
  - e.g., does vendor provide a security contact?
  - "Responsible disclosure" (a.k.a. "coordinated disclosure") generally covers this
- Includes product
  - E.g., does the advisory contain an advisory ID, specify affected versions, etc.?
  - CVRF indirectly covers this