McAfee
An Intel Company

Global Vulnerability Identification and Usage: A Vendor's Perspective

Kent Landfield
Director, Content Strategy, Architecture and Standards
McAfee Labs

Future of Global Vulnerability Reporting Summit
Kyoto 2012 FIRST Technical Colloquium
Kyoto, Japan
November, 13, 2012

SAFE NEVER SLEEPS™

Agenda

- Vendor Vulnerability Identification Uses

- Industry Vulnerability Identification Uses

- McAfee CVE Usage

- Current Problems with the Existing Vulnerability Landscape

- CVE Format Issues

- So what is really needed and why are we here?

Vendor Vulnerability Identification Usage

- Vulnerability Management Technologies
  - Detecting vulnerabilities in the deployed environment
  - Patching / remediating vulnerabilities
  - Reporting security posture status for organizational uses

- Vendor security related bulletins
  - Publishing
  - Compliance

- Information Key for security related databases
  - Research
  - Reporting

Industry Vulnerability Identification Usage

- Information Sharing between organizations or departments
  - Incident Handling
  - Operational security posture tracking
  - Security investment success
- Tracking method for use in determining the trending and scope of vulnerabilities
  - Costing
  - Awareness of the problem
- Common means to indicate that a single software vulnerability is a single condition
  - Unidentified vulnerabilities can appear as multiple problems when reported by multiple vendors

McAfee CVE Usage

- Customer Focused
  - Usage in our commercial products to assure the user’s have an understanding of what is in or not in their environments
  - Correlation of information for informing, displaying and reporting on vulnerability related issues

- Security Research
  - Extensive use as a primary key within our Compliance, Vulnerability, malware/malicious code and Global Threat Intelligence research environments
  - Common identifier that relates information between the teams
  - Metric for our coverage percentages for the individual products

- Common “language” for communicating vulnerabilities with our cooperating partners, Symantec, Trend, Cisco, HP, Microsoft and many, many others…

- And we are finding more uses on a very consistent basis…

Current Problems with the Existing Vulnerability Landscape

- Blind, Deaf and Dumb
  - CVE has been the foundational means for vulnerability identification
    - English speaking for the most part
  - Regional uses for vulnerability identification masks the problem
  - National / Regional means for identifying are lacking
    - Some are established and correlated with CVE
    - Some are immature in their process development
    - Some don’t exist at all
  - For the most part…. software vendors have been totally focused on CVE as the sole means for vulnerability identification
  - Large software development markets have no real established vulnerability identification programs that are visible to vendors and the regional community they were written for
  - Vendors can’t assist checking or correlating vulnerabilities they do not know about

CVE Format Issues

- Existing CVE format too small for English speaking vulnerability reporting today
- Limited to 10,000 vulnerabilities in a single year
  - CVE-YYYY-NNNN
- We have already exceeded that in the last couple years
  - Internal research data
- Do we simply add two digits to make it a 1,000,000 in a single year ?
  - CVE-YYYY-NNNNNN
  - Will that be enough for future uses ?
- We really need to keep it simple. What does that mean?
- What is the impact of format change on existing CVE support ?

So what is really needed and why are we here?

- The world is getting smaller by the year as the global network expands
- Security and network operations professionals / management need to be able to identify all vulnerabilities in their environment, regardless of what part of the world the software was written in.
- Vendors need a means to supply customers with the ability to determine a network's true vulnerability posture
- Security Research organizations need to know the complete landscape and not simply a portion of it
- CERTs and other Incident Handling organizations need to be able to deal with global issues consistently and effectively
- Need to extend CVE regardless as we are reaching the limits of the established CVE format
- Can we attack / solve two problems with one solution ?

McAfee®

An Intel Company