<table>
<thead>
<tr>
<th>The Common Vulnerability Reporting Framework (CVRF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presented by Jim Duncan, Juniper SIRT</td>
</tr>
<tr>
<td>FIRST Conference 2010, Miami FL USA</td>
</tr>
<tr>
<td>2010 June 15</td>
</tr>
</tbody>
</table>
Agenda

• What is CVRF?
• Why CVRF?
• Who built CVRF and how?
• What’s the value of CVRF?
• What’s the timeline?
• Which member companies will adopt CVRF?
• Q&A
What is CVRF?

• CVRF = the Common Vulnerability Reporting Framework

• XML-based language

• Provides a standard format for the dissemination of security-related information

• 48 Discrete Elements

• XML \(\rightarrow\) machine readable \(\rightarrow\) easier production and consumption
CVRF Roles

Document Producer
- Vendors
- Coordinators
- Researchers

Document Consumer
- Security Practitioners
- Administrators
- etc.
CVRF Roles: Document Producer
CVRF Roles: Document Consumer
Why CVRF?

• No existing standard in this unique vulnerability reporting space

• Others are ad hoc, producer-specific
Document Producer Reports at a Glance

**Cisco**
- Summary
- Affected Products
- Vulnerable Products
- Products Confirmed Not Vulnerable
- Details
- Vulnerability Scoring Details
- Impact
- Software Versions and Fixes
- Workarounds
- Obtaining Fixed Software
- Exploitation and Public Announcements
- Status of this Notice
- Distribution
- Revision History
- Cisco Security Procedures

**Microsoft**
- General Information
- Executive Summary
- Affected and Non-Affected Software
- Affected Software
- Non-Affected Software
- FAQ
- Vulnerability Information
- Severity Ratings and Vulnerability Identifiers
- 0 or more vulnerabilities sorted by CVE
- Vulnerability Description
- Update Information
- Detection and Deployment Tools Guidance
- Security Update Deployment
- Other Information
- Acknowledgements
- Microsoft Active Protections Program
- Support
- Disclaimer
- Revisions
## Document Producer Reports at a Glance, cont’d

**CERT**
- Target
- Access Vector
- Impact
- Remediation
- Details
- Impact
- Severity
- Vulnerability Coordination Information
- Vendor Information
- Remediation Information
- References
- Contact Information
- Revision History

**Secunia**
- Secunia Advisory
- Release Date
- Last Update Date
- Popularity
- Comments
- Criticality Level
- Impact
- Where
- Authentication Level
- Report Reliability
- Solution Status
- Systems Affected
- Approve Distribution
- Automated Scanning
- Operating System
- Secunia CVSS Score
- CVE References
- Description
- Solution
- Provided and/or Discovered by
- Changelog
- Original Advisory
- Other References
- Alternate/Detailed Remediation
- Deep links
Who’s involved?

- Internet Consortium for Advancement of Security on the Internet (ICASI)
- Formed in 2008 to address international, multi-product security challenges
- Non-profit, vendor agnostic
- ICASI members include Cisco, IBM, Intel, Juniper, Microsoft, and Nokia
- Non-ICASI member contributors include Oracle and Red Hat
How was CVRF built?

- Built a Best of Breed hypothetical model
- Took a baseline of industry vulnerability reports. Dissected, collated, performed gap analysis.
- Performed industry survey of end-users to find what is working and what isn’t.
- Re-Evaluate model
- Draft XML schema
- Re-factor company vulnerability reports in CVRF
- Submit for industry peer feedback. Is it cooked enough?
- Yes → Release CVRF 1.0
- No → We are here
What is the Value of CVRF?

• CVRF is a response by industry to customer demand

• Customers are looking for a simple automated way to absorb security-related information

• Vendors are looking for an easily produced capacity to enable machine readable generation of security documentation using current methodology

• CVRF is delivering the capacity to enable the assimilation of disparate security-related data-sets via a standard format
Timeline

- **2008**
  - Issue proposed as a goal for ICASI
  - CVRF work group formed
- **2009**
  - Investigation and gap analysis
  - Gathered reports from vendors and CERTs
  - Comparison with surveys
  - Draft problem statement and use cases
  - Design common Framework
- **2010**
  - Define standard
  - Develop dictionary, schema and sample style sheets
  - Test internal to working group
  - Conduct Peer review
  - Incorporate peer review comments
- **Late 2011**
  - Implementation
## Company Adoption

<table>
<thead>
<tr>
<th>Company</th>
<th>Plans</th>
<th>Role</th>
<th>Timeline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco</td>
<td>evaluating</td>
<td>producer</td>
<td>2011</td>
</tr>
<tr>
<td>IBM</td>
<td>limited support</td>
<td>producer/consumer</td>
<td>2011/12</td>
</tr>
<tr>
<td>Intel</td>
<td>limited support</td>
<td>producer/consumer</td>
<td>2011</td>
</tr>
<tr>
<td>Juniper</td>
<td>limited support</td>
<td>producer/consumer</td>
<td>2011/12</td>
</tr>
<tr>
<td>Microsoft</td>
<td>support</td>
<td>producer</td>
<td>2011</td>
</tr>
<tr>
<td>Nokia</td>
<td>evaluating</td>
<td>producer</td>
<td>2011</td>
</tr>
<tr>
<td>Oracle</td>
<td>evaluating</td>
<td>producer/consumer</td>
<td>2011/12</td>
</tr>
<tr>
<td>Red Hat</td>
<td>support</td>
<td>producer</td>
<td>2010</td>
</tr>
</tbody>
</table>
The “ask”:

• Well qualified organizations for Peer review

• Would your organization use an industry proposed framework to accomplish the purpose outlined here?

• Please email cvrf@icasi.org to request participation

• Other comments or questions?