The Risk Report

Ernest Park
ernest.park@airius.com
203-354-8800

Using SCAP Data to Output Time Sensitive Risk Analytics for FOSS

Copyright Airius Internet Solutions 2009
• **About Airius**
  ◦ Airius is an “Internet Company” created from Netscape to show the power of the internet for business.
  ◦ Originally developed solutions based on enterprise infrastructure
  ◦ New products aimed at delivery of objective information from distributed and unstructured data

• **Offerings:**
  ◦ GPL3 Search Site
  ◦ Risk Report

*A quick Google search will turn up Airius at Sun, AOL, and thousands of universities and enterprises that still use the original airius sample code*
The Problem

- National Vulnerability Database is structured as a list.
- Common Platform Enumeration (CPE) names are subjectively created.
- Data is not prioritized.
- Groups – families – of data are not merged (ie – Windows, Browsers, MySQL Database).
- CVE, CPE – like phonebooks of unrelated data.
- Chief Security Officers have Unpredictable Event Risk
- Compliance Officers have Governance and Policy Control Risk
- IT Management has Budget Risk
- Remove FUD – make decisions and present data based on timely facts
- Provide relational risk information for groups
- Objective data provides “best-practices” consulting daily

Who Cares – Users of NVD...
A list of standardized names for vulnerabilities and other information security exposures - CVE aims to standardize the names for all publicly known vulnerabilities and security exposures.

A Dictionary, NOT a Database - The goal of CVE is to make it easier to share data across separate vulnerability databases and security tools. While CVE may make it easier to search for information in other databases, CVE should not be considered as a vulnerability database on its own merit.

CVE is funded by the U.S. Department of Homeland Security.
http://nvd.nist.gov

NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. It is based on and synchronized with the CVE vulnerability naming standard.
Counting Cannon Balls
Sorted by Solution Type
NVD - now
71MBs of XML
NVD - now
Risk Report - Live

• Policies
• Preferences
• Inventory
• Research
• Subscription Management
• User Management
• Compliance Reports
• Open v. Resolved

Copyright Airius Internet Solutions 2009
risk_report@airius.com  203-354-8800
Proactive risk management


<XXXXXXX> - report update daily
RISK : Highest CVSS score within target report
WLI : workload index
New : number of new entries
Public Score : Highest relational score relative to the highest overall score
Updates : Preexisting CVEs with updated information
Patches : Number of CVEs with posted patches
Resolutions : Number of outstanding issues with verified resolutions (can include a patch)
XXXXXXX-19:22 EST – Timestamp of report

Sent to hand held devices, ticketing systems

Copyright Airius Internet Solutions 2009

rиск_report@airius.com  203-354-8800
### Supporting Data

<table>
<thead>
<tr>
<th>Date</th>
<th>CVE</th>
<th>Severity</th>
<th>Vendor</th>
<th>Applicat License</th>
<th>Description Status</th>
<th>CPE Name Affected</th>
<th>Patch Info</th>
<th>Patch Ver</th>
<th>Latest Rel</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXXXXX</td>
<td>CVE-2008-10</td>
<td>7.5</td>
<td>PCRE</td>
<td>PCRE</td>
<td>PCRE</td>
<td>allows corrupted</td>
<td><a href="http://nvd">http://nvd</a></td>
<td>7.7</td>
<td>none</td>
</tr>
<tr>
<td>XXXXXX</td>
<td>CVE-2008-10</td>
<td>7.5</td>
<td>Bluez</td>
<td>Bluez util</td>
<td>GNU GPL</td>
<td>allows rem updated</td>
<td><a href="http://nvd">http://nvd</a></td>
<td>3.35</td>
<td><a href="http://sec">http://sec</a></td>
</tr>
<tr>
<td>XXXXXX</td>
<td>CVE-2008-10</td>
<td>7.5</td>
<td>Bluez</td>
<td>Bluez util</td>
<td>GNU GPL</td>
<td>allows rem updated</td>
<td><a href="http://nvd">http://nvd</a></td>
<td>3.35</td>
<td><a href="http://sec">http://sec</a></td>
</tr>
<tr>
<td>XXXXXX</td>
<td>CVE-2008-10</td>
<td>7.5</td>
<td>Bluez</td>
<td>Bluez util</td>
<td>GNU GPL</td>
<td>allows rem updated</td>
<td><a href="http://nvd">http://nvd</a></td>
<td>3.35</td>
<td><a href="http://sec">http://sec</a></td>
</tr>
<tr>
<td>XXXXXX</td>
<td>CVE-2008-10</td>
<td>7.5</td>
<td>Bluez</td>
<td>Bluez util</td>
<td>GNU GPL</td>
<td>allows rem updated</td>
<td><a href="http://nvd">http://nvd</a></td>
<td>3.35</td>
<td><a href="http://sec">http://sec</a></td>
</tr>
<tr>
<td>XXXXXX</td>
<td>CVE-2008-10</td>
<td>7.5</td>
<td>Bluez</td>
<td>Bluez util</td>
<td>GNU GPL</td>
<td>allows rem updated</td>
<td><a href="http://nvd">http://nvd</a></td>
<td>3.35</td>
<td><a href="http://sec">http://sec</a></td>
</tr>
<tr>
<td>XXXXXX</td>
<td>CVE-2008-10</td>
<td>7.5</td>
<td>Bluez</td>
<td>Bluez util</td>
<td>GNU GPL</td>
<td>allows rem updated</td>
<td><a href="http://nvd">http://nvd</a></td>
<td>3.35</td>
<td><a href="http://sec">http://sec</a></td>
</tr>
</tbody>
</table>
Risks by Type: Database

Source - Airius Risk Report: 12/31/08

Copyright Airius Internet Solutions 2009

risk_report@airius.com  203-354-8800
CVEs by Type: Database

Source - Airius Risk Report: 12/31/08

Copyright Airius Internet Solutions 2009
CVEs by Type: Operating Systems

Source - Airius Risk Report: 12/31/08

Copyright Airius Internet Solutions 2009

risk_report@airius.com  203-354-8800
The Risk Management solution allows IT managers to receive time sensitive tactical information that they can act on immediately.

- The Risk Reporting Database
- Risk Update Report
- Customized Analytics

Risk Management does NOT detect. It focuses on a filtered, time sensitive alert function. It corrects naming issues and applies filtering by type and license.

Risk Report: Management
• Objective and time relevant information to drive decisions

• Diffuse the noise of “counting vulnerabilities”

• Replace noise with information

• Turn a fear metric into business rules
The Risk Report uses NVD data to assemble a hierarchical data structure with current and historical relevance.

- We layer *aliases, types, groups*, to provide more relevant reporting.
- The Airius Risk/Time score and the Airius Public score are ways to provide time relative and peer relative sorting of prioritized information.
- The output of the Risk Report is a customized data and graphs.

The Risk Report

Copyright Airius Internet Solutions 2009

risk_report@airius.com  203-354-8800
• Risk/Time Score metrics

• Considers TIME as a critical element when considering “current risk”, or risk as of right now.

• Provides a weighted metric to sort issues, riskiest being highest, relative to NOW.

• Sorts DANGER messages in a prioritized order of relevance. Cuts through the noise and makes sense of CVEs.

Using Time To Understand Risk

Copyright Airius Internet Solutions 2009

risk_report@airius.com  203-354-8800
Published: The Risk Report
The Risk Report - Top 25 FOSS

http://fossbazaar.org
Software risk is not just a cumulative measurement

- What, where, when
- Normal
  - Frequency
  - Severity
  - Duration
- Deviation from normal
- Relative time
- Risk management involves awareness of change

Risk: what, where, when
The Risk Report provides objective and time sensitive data for:

- **Performance Bonuses** – Recognizing achievement using objective metrics

- **Staffing** - Understanding, quantifying and measuring the operating requirements of risk management

- **Vendors** - Review and negotiation of support contracts with vendors using actual and historic data

- **Business Continuity/ Disaster Recovery** - Measuring security processes relative to actual risk

- **Objective Information** – Eliminate FUD and use reliable information to measure risk and market share

Manage Risk: Earn Rewards

risk_report@airius.com  203-354-8800
Risk Intelligence

*Products and Services focused on the timely delivery of accurate and relevant risk information*

- Integrating SCAP data into internal issue tracking
- Using objective and timely data to drive risk management policy
- Audit vendor/application risk
- Accurate and reliable statistics for management, external for marketing

Risk Intelligence
Mr. Park is a senior technology professional specializing in all the information around closed and open source software. He is the architect of the Risk Report, a real time analytic of reported vulnerabilities relative to products and releases.

Some of his published work can easily be recognized within the FOSS community. GPL3 search site; GPL3 blog; Working group member: CVE, CPE, DHS SwA; FOSS researcher; specialist in license and software usage and proliferation; Expert in creation and management of FOSS usage policy.

Mr. Park has delivered significant innovations specific to the use and identification of FOSS within enterprise environments. He is also an advocate for the development and maintenance of policies for the use of FOSS. Before his current work for Airius, Mr. Park acted as VP of Research for Palamida where he was credited with the creation of a number of significant innovations in the area of risk and license management specific to open source software.

Mr. Park works for Airius and can be retained for software (FOSS and commercial), license and risk management policy development and audit.

About Speaker: Ernest Park
• Time critical information for
  • Risk management
  • Staffing
  • Compensation
  • Business Continuity and
    Disaster Planning
• Customized reporting and
  advisory services available

Airius Internet Solutions
Ernest M. Park
e@airius.com
203-354-8800
203-856-7778

The end