

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

risk_report@airius.com 203-354-8800

- 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*



Airius Internet Solutions



Copyright Airius Internet Solutions 2009

risk_report@airius.com 203-354-8800

- 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



The Problem

Copyright Airius Internet Solutions 2009

- 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...



Common Vulnerabilities and Exposures

<http://cve.mitre.org>

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.

Vulnerability Standards





Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of
Standards and Technology

National Vulnerability Database

a comprehensive cyber vulnerability resource

<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.



Vulnerability Reporting

Copyright Airius Internet Solutions 2009

risk_report@airius.com 203-354-8800



Counting Cannon Balls



Copyright Airius Internet Solutions 2009

risk_report@airius.com 203-354-8800

Airius Risk Report

CUSTOM

Closed

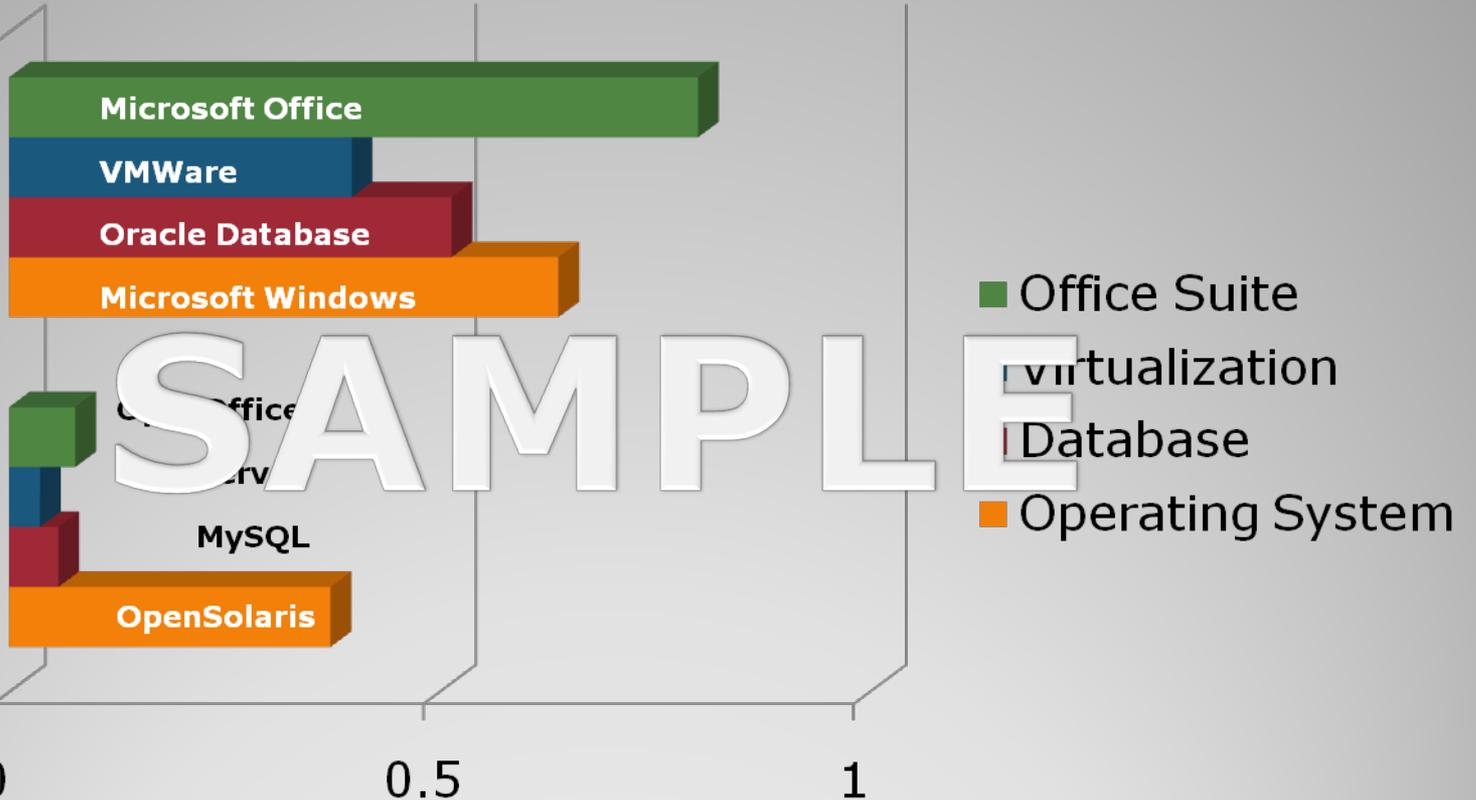
COSS

Airius Risk Score

0

0.5

1



Source - Airius Risk Report: 12/31/08



Relative Risk: COSS v. Closed

Copyright Airius Internet Solutions 2009

risk_report@airius.com 203-354-8800

Airius Risk Report

CUSTOM

Operating System

Microsoft Windows

OpenSolaris

Database

Oracle Database

MySQL

Office Suite

Microsoft Office

OpenOffice

Virtualization

VMWare

XenServer

Airius Risk Score

0.000

0.500

1.000

- Proprietary / Closed source
- Commercial Open source Software

SAMPLE

Source - Airius Risk Report: 12/31/08

Sorted by Solution Type



Book	Sheet	Name	Cell	Value
nvd-cve-2004.xml	nvd...	\$T\$527		Heap-based buffer overflo...
nvd-cve-2004.xml	nvd...	\$A\$15529		http://otn.oracle.com/depl...
nvd-cve-2004.xml	nvd...	\$A\$15529		http://otn.oracle.com/depl...
nvd-cve-2004.xml	nvd...	\$A\$15530		oracle-web-cache-vulnera...
nvd-cve-2004.xml	nvd...	\$A\$15533		20040316 new security al...

P	Q
5497	2004-0109
5498	2004-0109
5499	2004-0109
5500	2004-0109
5501	2004-0109
5502	2004-0109
5503	2004-0109
5504	2004-0109
5505	2004-0109
5506	2004-0109
5507	2004-0109
5508	2004-0109
5509	2004-0109
5510	2004-0109
5511	2004-0109
5512	2004-0109
5513	2004-0109
5514	2004-0109
5515	2004-0109
5516	2004-0109
5517	2004-0109
5518	2004-0109
5519	2004-0109
5520	2004-0109
5521	2004-0109
5522	2004-0109
5523	2004-0109
5524	2004-0109
5525	2004-0109
5526	2004-0109
5527	2004-0385
5528	2004-0385

```

Documents\My Projects\Risk Report\cpe\s\nvd xml\new - 022409\output\nvd-cve-2005.xml]
View Format Column Macro Scripting Advanced Window Help
CVE-2009-0238
0 10 20 30 40 50 60
23304 <refs>
23305 <ref source="CONFIRM" patch="1" url="http://kernel.or
23306 <ref source="UBUNTU" url="http://www.ubuntulinux.org/
23307 <ref source="BID" url="http://www.securityfocus.com/b
23308 <ref source="FEDORA" url="http://www.securityfocus.co
23309 <ref source="SUSE" url="http://www.securityfocus.com/
23310
23311
23312
23313
23314
23315
23316
23317
23318
23319
23320
23321
23322
23323
23324 <vers num="2.6.11.12" />
23325 <vers num="2.6.11.2" />
23326 <vers num="2.6.11.3" />
23327 <vers num="2.6.11.4" />
23328 <vers num="2.6.11.5" />
23329 <vers num="2.6.11.6" />
23330 <vers num="2.6.11.7" />
Ln 123314, Col. 18, C0 DOS XML Mod: 3/12/2009 4:20:06 AM File Size: 9768120
  
```

Find

Find What: oracle

179 occurrences found.

Match Whole Word Or
 Match Case
 Regular Expressions

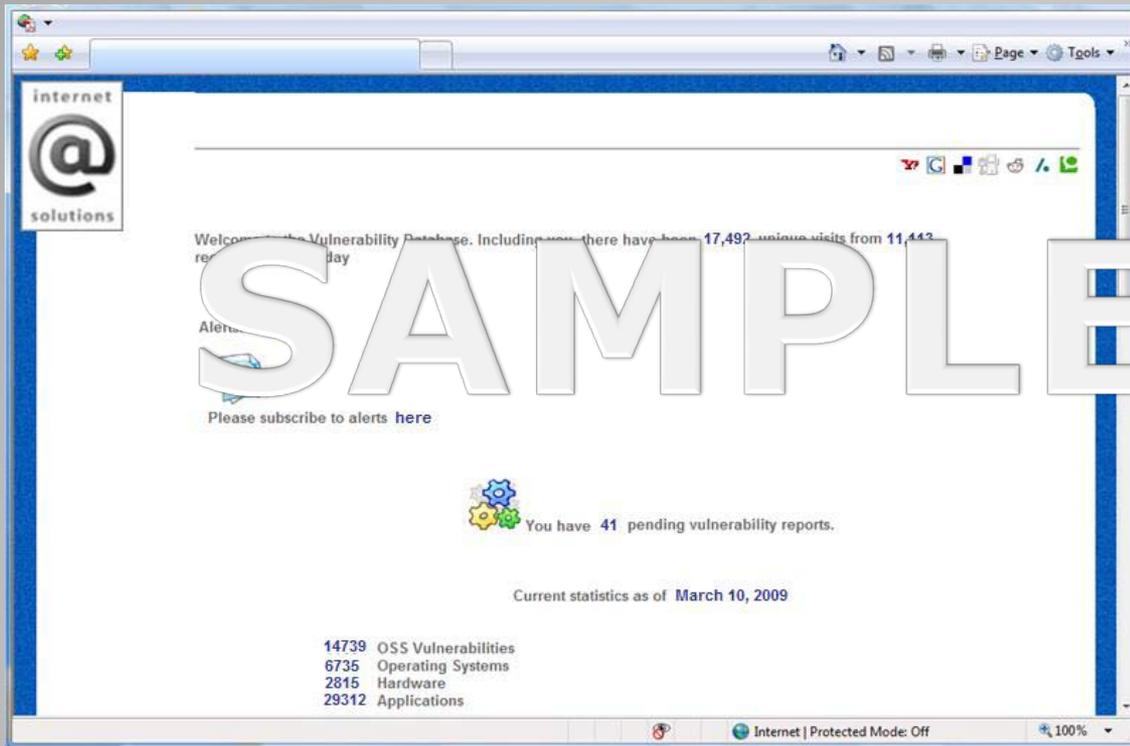
Next Previous Count All Close Help Advanced

71 MBs of XML

NVD - now



Risk Report - Live



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

Risk Report - LIVE



Risk Report - Live

Sent to hand held devices, ticketing systems

Risk Report for < XXXXXXXX > RISK 10 - WLI 9.63 - 4 new - 97% public score - 59 updates - 47 patches - 48 resolutions - XXXXXXXX-19:22 EST

SAMPLE

<XXXXXXXXXX> refresh rate 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)

XXXXXXXXXX-19:22 EST – Timestamp of report



Proactive risk management

Risk Report - Live

Supporting Data

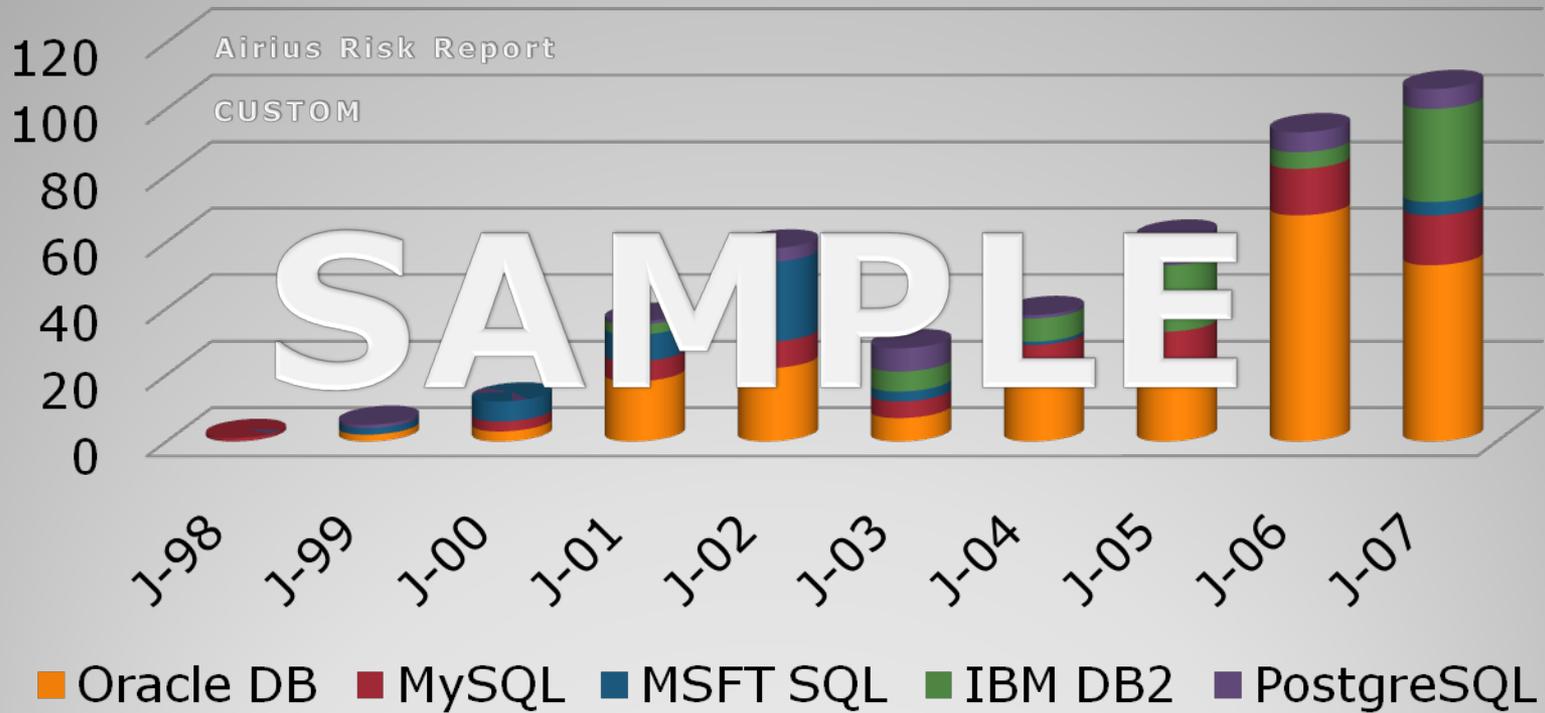
Date	CVE	Severity	Vendor	Applicatic License	Descriptio Status	CPE Name Affected	Patch Info	Patch Ver.	Latest Rel
XXXXXXXX	CVE-2008-	7.5	PCRE	PCRE Lice	allows con updated	http://nvd	7.7	none	7.7
XXXXXXXX	CVE-2008-	7.5	Bluez	Bluez libs GNU GPL	allows rem updated	http://nvd	3.30, and	http://sec	3.35
XXXXXXXX	CVE-2008-	7.5	Bluez	Bluez util GNU GPL	allows rem updated	http://nvd	3.33, and	http://sec	3.35
XXXXXXXX	CVE-2008-	7.5	Sub	GNU GP	allows rem updated	http://nvd	and	none	11
XXXXXXXX	CVE-2008-	7.5	Mozilla	Firefox MPL/GPL	allows rem updated	http://nvd	before2	http://sec	2.0
XXXXXXXX	CVE-2008-	10	Mozilla	Firefox MPL/GPL	allows rem updated	http://nvd	before 1.	http://ww	1.1
XXXXXXXX	CVE-2008-	10	Mozilla	Firefox MPL/GPL	allows rem updated	http://nvd	before 2.0.0.14	none	2.0.0.14
XXXXXXXX	CVE-2008-	10	Mozilla	Seamonke MPL/GPL	allow rem updated	http://nvd	before 1.1	http://ww	1.1.0
XXXXXXXX	CVE-2008-	10	Mozilla	Thunderb MPL/GPL	allow rem updated	http://nvd	2.0.0.14ar	none	2.0.0.14
XXXXXXXX	CVE-2008-	4.3	Mozilla	Firefox MPL/GPL	allow rem updated	http://nvd	before2.0	http://ww	2.0.0.15
XXXXXXXX	CVE-2008-	4.3	Mozilla	Seamonke MPL/GPL	allow rem updated	http://nvd	before 1.1	http://ww	1.1.0
XXXXXXXX	CVE-2008-	7.5	Mozilla	Firefox MPL/GPL	allows rem updated	http://nvd	before2.0	http://ww	2.0.0.15
XXXXXXXX	CVE-2008-	7.5	Mozilla	Seamonke MPL/GPL	allows rem updated	http://nvd	before 1.1	http://ww	1.1.0
XXXXXXXX	CVE-2008-	7.5	Mozilla	Firefox MPL/GPL	allow rem updated	http://nvd	before2.0	http://ww	2.0.0.15
XXXXXXXX	CVE-2008-	7.5	Mozilla	Seamonke MPL/GPL	allow rem updated	http://nvd	before 1.1	http://ww	1.1.0
XXXXXXXX	CVE-2008-	7.5	Mozilla	Thunderb MPL/GPL	allows rem updated	http://nvd	2.0.0.14ar	none	2.0.0.14
XXXXXXXX	CVE-2008-	7.5	Mozilla	Firefox MPL/GPL	allows rem updated	http://nvd	before2.0	http://ww	2.0.0.15
XXXXXXXX	CVE-2008-	5	Mozilla	Seamonke MPL/GPL	allow rem updated	http://nvd	before 1.1	http://ww	1.1.0
XXXXXXXX	CVE-2008-	7.5	Mozilla	Firefox MPL/GPL	allow rem updated	http://nvd	before2.0	http://ww	2.0.0.15

SAMPLE



Proactive risk management

Risk Report: 10yr Databases



Source - Airius Risk Report: 12/31/08

CVEs by Type: Database



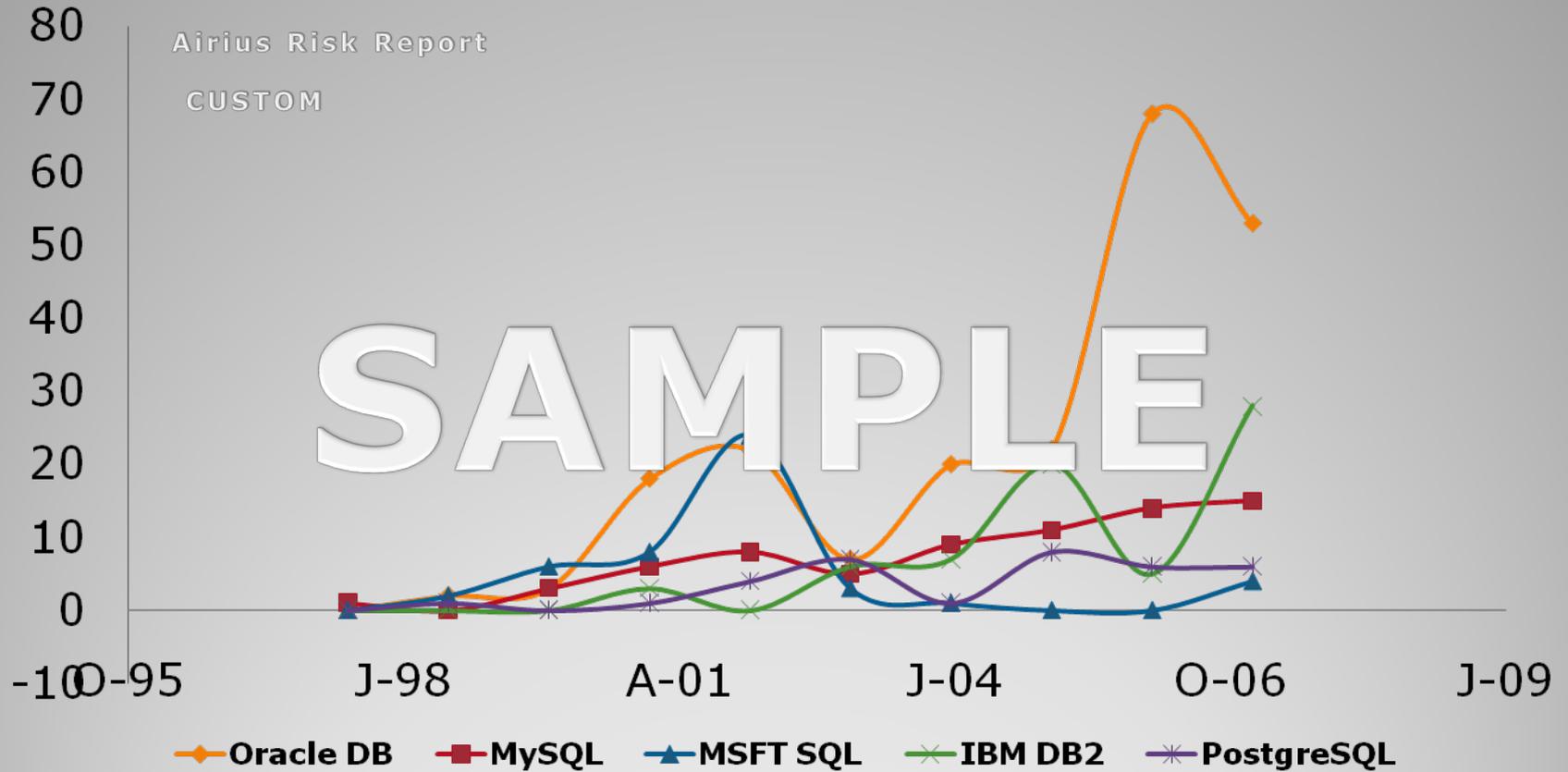
Copyright Airius Internet Solutions 2009

risk_report@airius.com 203-354-8800

Airius Risk Report

CUSTOM

SAMPLE



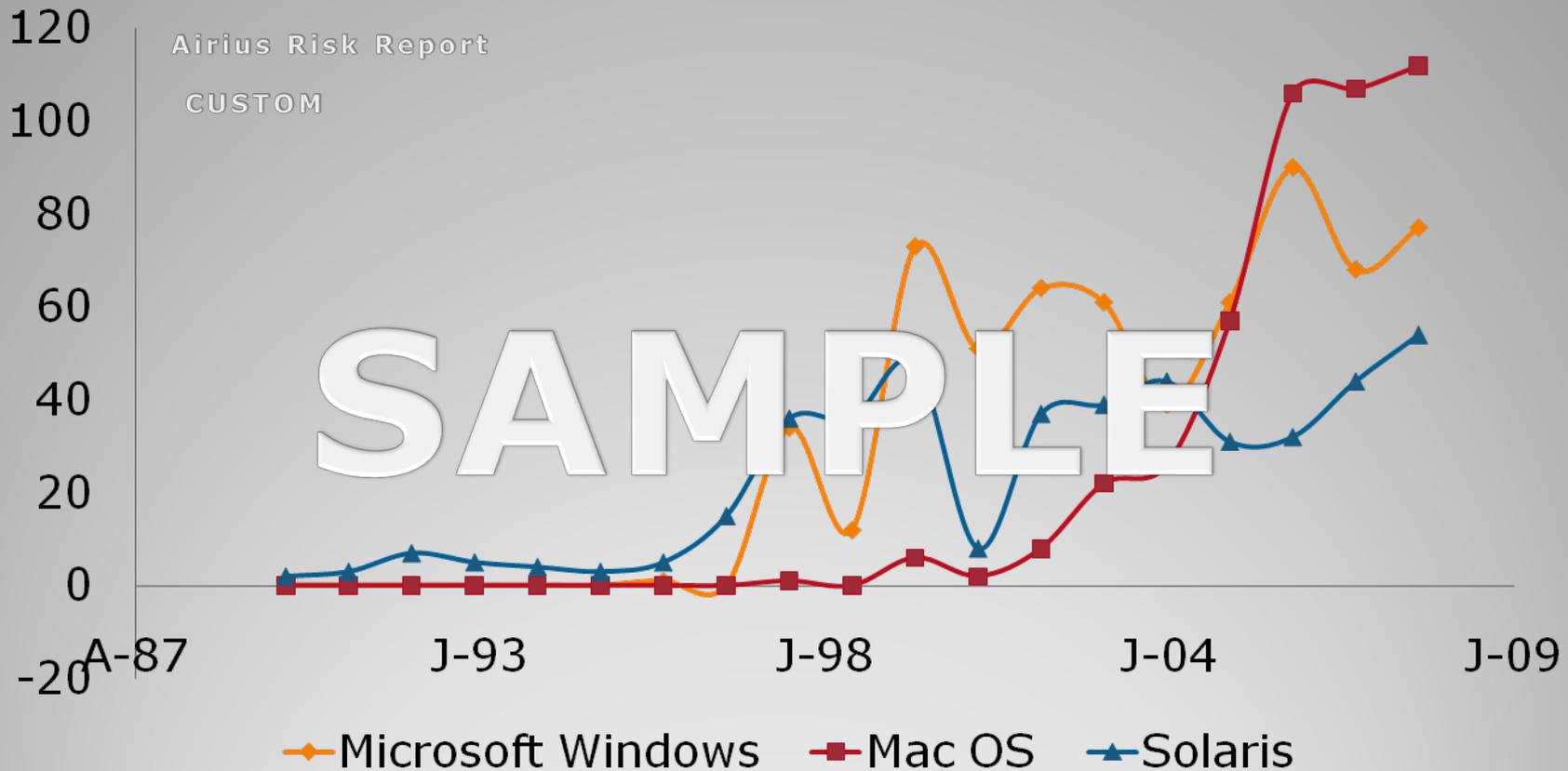
Source - Airius Risk Report: 12/31/08

CVEs by Type: Database



Copyright Airius Internet Solutions 2009

risk_report@airius.com 203-354-8800



Source - Airius Risk Report: 12/31/08

CVEs by Type: Operating Systems



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

Risk Intelligence



- 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



• 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



CVSS – 8,
today

CVSS – 9, 14
days ago

CVSS – 7, 30
days ago

CVSS – 10,
120 days ago

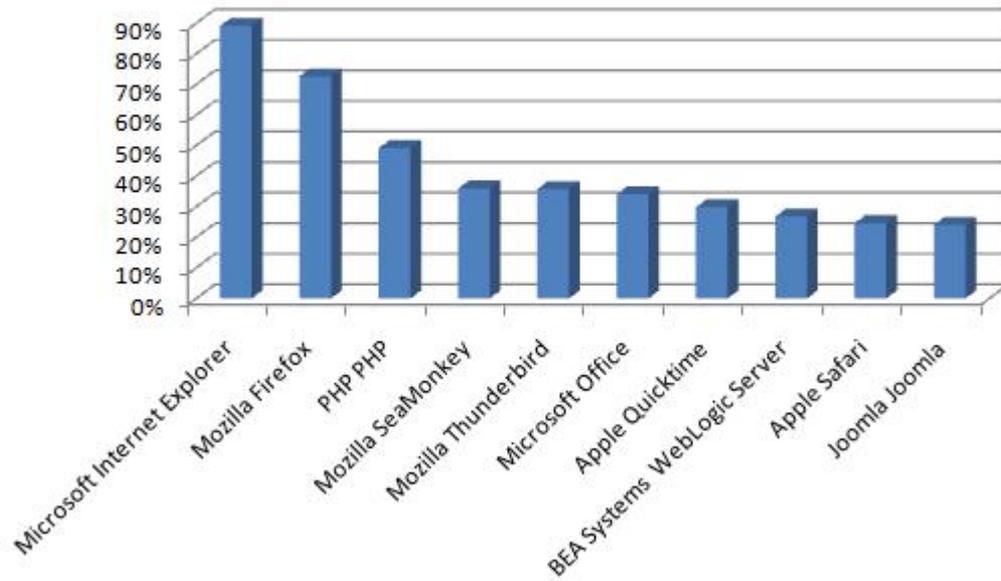


Using Time To Understand Risk



2008: The Risk Report - Top 10 Apps

risk_report@airius.com 1/13/09



"The Risk Report", copyright 2009, Airius Internet Solutions *risk_report@airius.com*



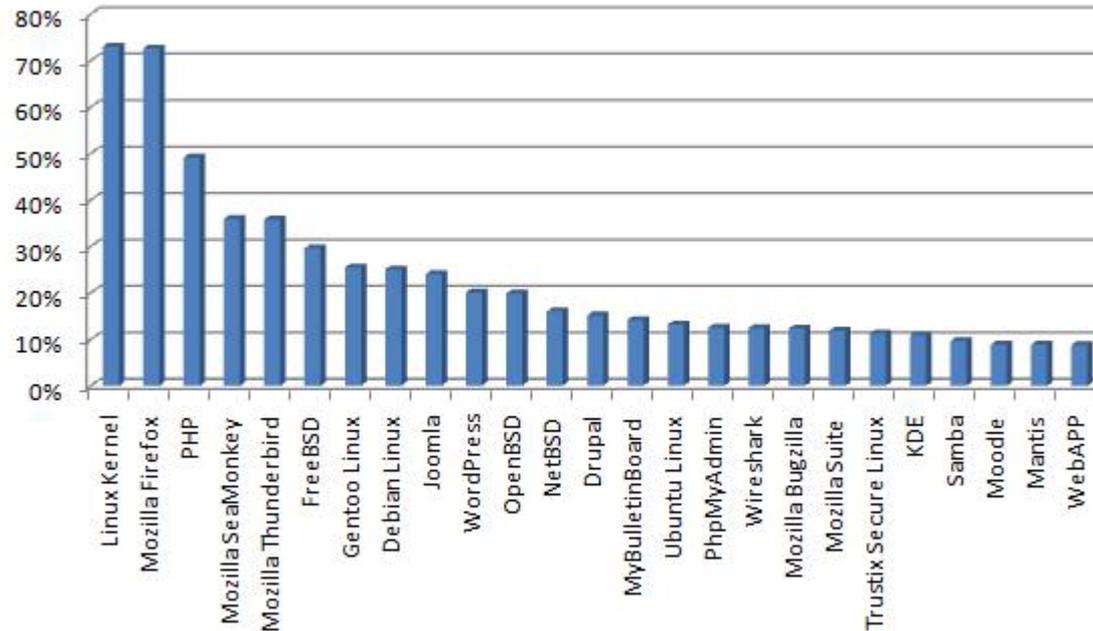
Published: The Risk Report

Copyright Airius Internet Solutions 2009

risk_report@airius.com 203-354-8800

The Risk Report - Top 25 FOSS

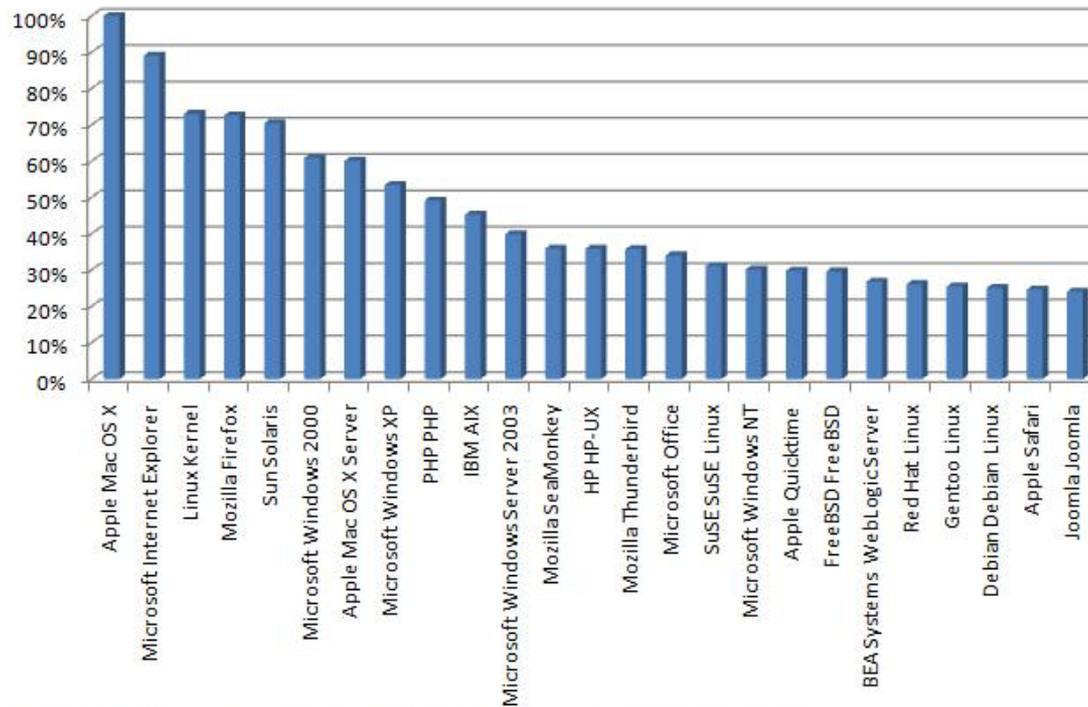
risk_report@airius.com 01/16/09



"The Risk Report", copyright 2009, Airius Internet Solutions risk_report@airius.com

2008: The Risk Report - Top 25

risk_report@airius.com 1/13/09



"The Risk Report", copyright 2009, Airius Internet Solutions risk_report@airius.com



<http://gpl3.blogspot.com>

Copyright Airius Internet Solutions 2009

risk_report@airius.com 203-354-8800

- 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 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



Copyright Airius Internet Solutions 2009

risk_report@airius.com 203-354-8800

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

Copyright Airius Internet Solutions 2009

risk_report@airius.com 203-354-8800