

Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

Product Focus

[Sasser Worm Scanner](#) - The S4 Sasser Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the Microsoft SSL Vulnerability (MS04-011) that used by the Sasser Worm to infect machines.

Download Here:

<http://www.netvigilance.com/productdownloads?productname=sasserwormscanner>

This Week in Review

Security spendings expected to increase. How to best protect your computer. Hacking on the rise. Phishing on the rise.

Enjoy reading & Stay safe.

Call or email netVigilance to get an update on SecureScout.

(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

• Despite downturn, IT security spending to increase

Management increasingly is recognizing security as a top business priority, which is resulting in higher budgets for some organizations despite the economic slowdown, according to a new survey.

The survey from the Computer Technology Industry Association (CompTIA), an IT trade group, compiled the responses of 1,538 organizations of varying sizes in the United, Canada, India, UK and China.

According to the survey, regardless of region, the mean spending for security-related technologies now is \$719,930, an increase of 20 percent compared to last year.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Despite-downturn-IT-security-spending-to-increase/article/130550/>

• Security Software: Protection or Extortion?

April 14, 2009 (PC World) As the Conficker worm sprang to life on April 1, talk here at the PC World offices turned to some interesting debates about how best to protect PCs from malware threats. In recent weeks we've run several helpful articles offering tips, tricks, and insights to keep you and your PC safe from Conficker and other malware on the Internet. At the same time, a few among us have revealed that they don't run any security software at all on their own machines--and have no intention of starting now.

Is he insane? Naïve? To find out, we gave Rick a podium to speak on behalf of those who shrug off the safety of antimalware suites, and to defend his point of view in a debate with security correspondent Robert Vamosi, who regularly reports on malware and other security threats for PC World's Business Center. Who's right? Who's nuts? You be the judge. Share your view in our comments section.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9131551&source=rss_topic1

• Criminals exploit careless mistakes as data breaches hit record

In a study of large-scale data breaches in 2008, Verizon Business found that cybercriminals profited mostly from exploiting careless mistakes.

"The overall message about hacking in 2008 was that it was not all that sophisticated," Wade Baker, research and intelligence principal, Verizon Business, and primary author of the report, told SCMagazineUS.com Wednesday. "The criminals are getting in the door through very low-level means. They are not having to work hard to get in the door. But once they are there, they begin to do some very sophisticated things."

The study also revealed the intricate methodology and sophistication of recent attacks.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Criminals-exploit-careless-mistakes-as-data-breaches-hit-record/article/130700/>

• Phishing increased 40 percent in 2008

The percentage of people losing money to phishing attacks is higher than ever -- 5 million consumers in the U.S. fell victim during 2008, an increase of 40 percent over 2007, according to a new report put out by Gartner called "The war on phishing is far from over."

"You can't relax, you have to assume phishing emails are getting through -- they are," Avivah Litan, vice president and distinguished analyst at Gartner who authored the report told SCMagazineUS.com Wednesday.

Gartner conducted a survey of 3,985 individuals in September 2008 to determine consumer phishing trends. According to the survey, 4.26 percent of those who received phishing emails lost money from the scam (compared to 2.97 in 2005). Litan said that a 4 percent successful response rate is quite good, considering legitimate mass email marketing campaigns have a success rate of about 1.5 percent.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Phishing-increased-40-percent-in-2008/article/130702/>

New Vulnerabilities Tested in SecureScout

• 13693 Oracle Database Server - Resource Manager component unspecified Vulnerability (apr-2009/CVE-2009-0979)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Resource Manager" component.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>

* SECUNIA: 34693

<http://secunia.com/advisories/34693/>

CVE Reference:

CVE-2009-0979 (cve.mitre.org, nvd.nist.gov)

• 13694 Oracle Database Server - Core RDBMS component unspecified Vulnerability (apr-2009/CVE-2009-0985)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Core RDBMS" component.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>

* SECUNIA: 34693

<http://secunia.com/advisories/34693/>

CVE Reference:

CVE-2009-0985 (cve.mitre.org, nvd.nist.gov)

• 13695 Oracle Database Server - Workspace Manager component unspecified Vulnerability (apr-2009/CVE-2009-0972)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Workspace Manager" component.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>

* SECUNIA: 34693

<http://secunia.com/advisories/34693/>

CVE Reference:

CVE-2009-0972 (cve.mitre.org, nvd.nist.gov)

• 13696 Oracle Database Server - Advanced Queuing component unspecified Vulnerability (apr-2009/CVE-2009-0977)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Advanced Queuing" component.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>

* SECUNIA: 34693

<http://secunia.com/advisories/34693/>

CVE Reference:

CVE-2009-0977 (cve.mitre.org, nvd.nist.gov)

• 13697 Oracle Database Server - Advanced Queuing component unspecified Vulnerability (apr-2009/CVE-2009-0992)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Advanced Queuing" component.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>

* SECUNIA: 34693

<http://secunia.com/advisories/34693/>

CVE Reference:

CVE-2009-0992 (cve.mitre.org, nvd.nist.gov)

• 13698 Oracle Database Server - Database Vault component unspecified Vulnerability (apr-2009/CVE-2009-0984)

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Database Vault" component.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>
- * SECUNIA: 34693
<http://secunia.com/advisories/34693/>

CVE Reference:

CVE-2009-0984 (cve.mitre.org, nvd.nist.gov)

• **13699 Oracle Database Server - SQLX Functions component unspecified Vulnerability (apr-2009/CVE-2009-0980)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "SQLX Functions" component.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>
- * SECUNIA: 34693
<http://secunia.com/advisories/34693/>

CVE Reference:

CVE-2009-0980 (cve.mitre.org, nvd.nist.gov)

• **13700 Oracle Database Server - Workspace Manager component unspecified Vulnerability (apr-2009/CVE-2009-0975)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Workspace Manager" component.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>
- * SECUNIA: 34693
<http://secunia.com/advisories/34693/>

CVE Reference:

CVE-2009-0975 (cve.mitre.org, nvd.nist.gov)

• **13701 Oracle Database Server - Workspace Manager component unspecified Vulnerability (apr-2009/CVE-2009-0976)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Workspace Manager" component.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

References:

- * CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>
- * SECUNIA: 34693
<http://secunia.com/advisories/34693/>

CVE Reference:

CVE-2009-0976 (cve.mitre.org, nvd.nist.gov)

• **13702 Oracle Database Server - Workspace Manager component unspecified Vulnerability (apr-2009/CVE-2009-0978)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Workspace Manager" component.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

References:

* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>

* SECUNIA: 34693

<http://secunia.com/advisories/34693/>

CVE Reference:

CVE-2009-0978 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-0086 Microsoft CVSS 2.0 Score = 10.0

Integer underflow in Windows HTTP Services (aka WinHTTP) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote HTTP servers to execute arbitrary code via crafted parameter values in a response, related to error handling, aka "Windows HTTP Services Integer Underflow Vulnerability."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-013.msp>

CVE Reference: [CVE-2009-0086](#)

• CVE-2009-0088 Microsoft CVSS 2.0 Score = 10.0

The WordPerfect 6.x Converter in Microsoft Office Word 2000 SP3 and Microsoft Office Converter Pack does not properly validate the length of an unspecified string, which allows remote attackers to execute arbitrary code via a crafted WordPerfect 6.x file, aka "Word 2000 WordPerfect 6.x Converter Stack Corruption Vulnerability."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-010.msp>

CVE Reference: [CVE-2009-0088](#)

• CVE-2009-0084 Microsoft CVSS 2.0 Score = 9.3

DirectShow in Microsoft DirectX 8.1 and 9.0 does not properly decompress media files, which allows remote attackers to execute arbitrary code via a crafted MJPEG (1) file or (2) video stream, aka "MJPEG Decompression Vulnerability."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-011.msp>

CVE Reference: [CVE-2009-0084](#)

• CVE-2009-0087 Microsoft CVSS 2.0 Score = 9.3

Unspecified vulnerability in the Word 6 text converter in WordPad in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2; and the Word 6 text converter in Microsoft Office Word 2000 SP3 and 2002 SP3; allows remote attackers to execute arbitrary code via a crafted Word 6 file that contains malformed data, aka "WordPad and Office Text Converter Memory Corruption Vulnerability."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-010.msp>

CVE Reference: [CVE-2009-0087](#)

• CVE-2009-0100 Microsoft CVSS 2.0 Score = 9.3

Microsoft Office Excel 2000 SP3, 2002 SP3, 2003 SP3, and 2007 SP1; Excel in Microsoft Office 2004 and 2008 for Mac; Microsoft Office Excel Viewer and Excel Viewer 2003 SP3; and Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 do not properly parse the Excel spreadsheet file format, which allows remote attackers to execute arbitrary code via a crafted spreadsheet that contains a malformed object, aka "Memory Corruption Vulnerability."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-009.msp>

CVE Reference: [CVE-2009-0100](#)

• **CVE-2009-0235 Microsoft CVSS 2.0 Score = 9.3**

Stack-based buffer overflow in the Word 97 text converter in WordPad in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via a crafted Word 97 file that triggers memory corruption, aka "WordPad Word 97 Text Converter Stack Overflow Vulnerability."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-010.msp>

CVE Reference: [CVE-2009-0235](#)

• **CVE-2009-0550 Microsoft CVSS 2.0 Score = 9.3**

Windows HTTP Services (aka WinHTTP) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008; and WinINet in Microsoft Internet Explorer 5.01 SP4, 6 SP1, 6 and 7 on Windows XP SP2 and SP3, 6 and 7 on Windows Server 2003 SP1 and SP2, 7 on Windows Vista Gold and SP1, and 7 on Windows Server 2008; allows remote web servers to capture and replay NTLM credentials, and execute arbitrary code, via vectors related to absence of a "credential-reflection protections" opt-in step, aka "Windows HTTP Services Credential Reflection Vulnerability" and "WinINet Credential Reflection Vulnerability."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-014.msp>

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-013.msp>

CVE Reference: [CVE-2009-0550](#)

• **CVE-2009-0551 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 6 SP1, 6 and 7 on Windows XP SP2 and SP3, 6 and 7 on Windows Server 2003 SP1 and SP2, 7 on Windows Vista Gold and SP1, and 7 on Windows Server 2008 does not properly handle transition errors in a request for one HTTP document followed by a request for a second HTTP document, which allows remote attackers to execute arbitrary code via vectors involving (1) multiple crafted pages on a web site or (2) a web page with crafted inline content such as banner advertisements, aka "Page Transition Memory Corruption Vulnerability."

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-014.msp>

CVE Reference: [CVE-2009-0551](#)

Vulnerability Resource

Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the 'security portal for information system security professionals' is well founded. <http://www.infosyssec.org/infosyssec/>

Thank You

Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at ScoutNews@netVigilance.com

About SecureScout

SecureScout is a leading vulnerability scanner and management tool developed and marketed worldwide by NexantiS Corporation.

SecureScout is a trademark of NexantiS Corporation.

netVigilance, Inc. is a partner of NexantiS and an authorized distributor of SecureScout.

For any inquiry about SecureScout by:

Customers in America and Northern Europe contact us at info@netVigilance.com

Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at info-scanner@securescout.net