

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

[CodeRed Worm Scanner](#) - The S4 CodeRed Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any have been infected by CodeRed Worm.

Download Here:

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

This Week in Review

Cloud to grow immensely. Mobile malware expected to take off. Another group of hackers charged. Websites still too vulnerable.

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

- **SC eConference and Expo: Cloud computing speaker discusses risks to businesses and offers suggestions**

Cloud computing is going strong. In fact, research firm Gartner predicts that worldwide revenues for cloud services will grow from some \$46 billion in 2008 to approximately \$150 billion in 2013.

But along with this growth comes questions about how corporate data in the cloud will stay secure.

Bob West, CEO and founder of consultancy Echelon One, who spoke on a panel during Tuesday's live SC Magazine "Securing the Cloud" eConference and Expo, said there are many questions that security pros should pose to their cloud providers before entrusting data to them. SC Magazine

Full Story :

<http://www.scmagazineus.com/SC-eConference-and-Expo-Cloud-computing-speaker-discusses-risks-to-businesses>

- **Remote repair for infected phones in development**

In response to the growing threat of mobile malware, researchers at Georgia Tech are planning to study mobile device security and ultimately hope to devise a way to remotely repair infected devices. "Today, there haven't been widespread attacks, but we are seeing attackers starting to pay attention to mobile devices and we expect that that's only going to be increasing," Jonathon Giffin, an assistant computer science professor, told SCMagazineUS.com on Tuesday.

Giffin and fellow assistant professor Patrick Traynor will lead a research study into cyberattacks within cellular networks, to be funded by a three-year, \$450,000 grant from the National Science Foundation.

The researchers and a team of graduate students plan to build a cellular network test bed on campus to simulate how cellular devices communicate, Giffin said. Subsequently, they plan to study how attacks against mobile devices operate inside the test bed. SC Magazine

Full Story :

<http://www.scmagazineus.com/Remote-repair-for-infected-phones-in-development/article/157504/>

• Eastern Europeans charged in payment processor hack

(Credit: U.S. Department of Justice)

A group of Eastern Europeans was charged with hacking into the network of payment processor RBS WorldPay and using counterfeit debit cards at ATMs around the world to steal more than \$9 million, the U.S. Justice Department said on Tuesday.

Four of the defendants allegedly collaborated to break into the RBS WorldPay network on November 4, 2008, where they got access to the account numbers for prepaid payroll cards used by employees to withdraw salaries from ATMs, according to the indictment from a federal grand jury in Atlanta. The defendants allegedly reverse-engineered the PINs associated with the accounts from the encrypted data on the network. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-10394558-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• Study finds 64 percent of websites contain serious flaws

While a number of trusted sources continually decry the vulnerabilities present in web applications, this vector remains the primary avenue of attack for cybercriminals, according to a WhiteHat Website Security Statistics Report released on Thursday.

Despite metrics that substantiate the claims and any number of security best practices recommendations, many organizations, particularly those building custom web applications, are at risk, says the report, which measured data collected from Jan. 1, 2006 to Oct. 1, 2009, across more than 1,300 websites.

The problem is exacerbated because it is not possible to patch against custom web application software, such as that used by big e-commerce sites, Jeremiah Grossman, founder and CTO of WhiteHat, told SCMagazineUS.com. And that, he said, includes the vast majority of sites. SC Magazine

Full Story :

http://www.scmagazineus.com/Study-finds-64-percent-of-websites-contain-serious-flaws/article/157655/?utm_source

New Vulnerabilities Tested in SecureScout

• 18588 Win32k NULL Pointer Dereferencing Vulnerability (MS09-065/969947) (Remote File Checking)

An elevation of privilege vulnerability exists because the Windows kernel does not properly validate an argument passed to a Windows kernel system call. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* MS: MS09-065

<http://www.microsoft.com/technet/security/Bulletin/MS09-065.msp>

* BID: 36939

<http://www.securityfocus.com/bid/36939>

* VUPEN: VUPEN/ADV-2009-3191

<http://www.vupen.com/english/advisories/2009/3191>

* SECTRACK: 1023155

<http://securitytracker.com/alerts/2009/Nov/1023155.html>

CVE Reference:

CVE-2009-1127 (cve.mitre.org, nvd.nist.gov)

• **18589 Win32k Insufficient Data Validation Vulnerability (MS09-065/969947) (Remote File Checking)**

An elevation of privilege vulnerability exists in Windows kernel-mode drivers due to improper validation of input passed from user mode through the kernel component of GDI. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* MS: MS09-065

<http://www.microsoft.com/technet/security/Bulletin/MS09-065.msp>

* BID: 36941

<http://www.securityfocus.com/bid/36941>

* VUPEN: VUPEN/ADV-2009-3191

<http://www.vupen.com/english/advisories/2009/3191>

* SECTRACK: 1023155

<http://securitytracker.com/alerts/2009/Nov/1023155.html>

CVE Reference:

CVE-2009-2513 (cve.mitre.org, nvd.nist.gov)

• **18590 Win32k EOT Parsing Vulnerability (MS09-065/969947) (Remote File Checking)**

A remote code execution vulnerability exists in the Windows kernel-mode drivers due to the improper parsing of font code when building a table of directory entries. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

* MS: MS09-065

<http://www.microsoft.com/technet/security/Bulletin/MS09-065.msp>

* BID: 36029

<http://www.securityfocus.com/bid/36029>

* VUPEN: VUPEN/ADV-2009-3191

<http://www.vupen.com/english/advisories/2009/3191>

* SECTRACK: 1023155

<http://securitytracker.com/alerts/2009/Nov/1023155.html>

CVE Reference:

CVE-2009-2514 (cve.mitre.org, nvd.nist.gov)

• **18591 Excel Cache Memory Corruption Vulnerability (MS09-067/972652) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel files. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

* MS: MS09-067

<http://www.microsoft.com/technet/security/Bulletin/MS09-067.msp>

* BID: 36943

<http://www.securityfocus.com/bid/36943>

* VUPEN: VUPEN/ADV-2009-3193

<http://www.vupen.com/english/advisories/2009/3193>

* SECTRACK: 1023157

<http://securitytracker.com/alerts/2009/Nov/1023157.html>

CVE Reference:

CVE-2009-3127 (cve.mitre.org, nvd.nist.gov)

• 18592 Excel SxView Memory Corruption Vulnerability (MS09-067/972652) (Remote File Checking)

A remote code execution vulnerability exists in the way Microsoft Office Excel handles specially crafted Excel files that include a malformed record object. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

- * MS: MS09-067
<http://www.microsoft.com/technet/security/Bulletin/MS09-067.msp>
- * BID: 36944
<http://www.securityfocus.com/bid/36944>
- * VUPEN: VUPEN/ADV-2009-3193
<http://www.vupen.com/english/advisories/2009/3193>
- * SECTRACK: 1023157
<http://securitytracker.com/alerts/2009/Nov/1023157.html>

CVE Reference:

CVE-2009-3128 (cve.mitre.org, nvd.nist.gov)

• 18593 Excel Featheader Record Memory Corruption Vulnerability (MS09-067/972652) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel handles specially crafted Excel files that include a malformed record object. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

- * MS: MS09-067
<http://www.microsoft.com/technet/security/Bulletin/MS09-067.msp>
- * BID: 36945
<http://www.securityfocus.com/bid/36945>
- * VUPEN: VUPEN/ADV-2009-3193
<http://www.vupen.com/english/advisories/2009/3193>
- * SECTRACK: 1023157
<http://securitytracker.com/alerts/2009/Nov/1023157.html>

CVE Reference:

CVE-2009-3129 (cve.mitre.org, nvd.nist.gov)

• 18594 Excel Document Parsing Heap Overflow Vulnerability (MS09-067/972652) (Remote File Checking)

A remote code execution vulnerability exists in the way Microsoft Office Excel handles specially crafted Excel files with malformed BIFF records. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

- * MS: MS09-067
<http://www.microsoft.com/technet/security/Bulletin/MS09-067.msp>
- * BID: 36946
<http://www.securityfocus.com/bid/36946>
- * VUPEN: VUPEN/ADV-2009-3193
<http://www.vupen.com/english/advisories/2009/3193>
- * SECTRACK: 1023157
<http://securitytracker.com/alerts/2009/Nov/1023157.html>

CVE Reference:

CVE-2009-3130 (cve.mitre.org, nvd.nist.gov)

• 18595 Excel Formula Parsing Memory Corruption Vulnerability (MS09-067/972652) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Office Excel parses documents containing a specially crafted formula embedded inside a cell. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights in the context of the currently logged on user.

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

References:

- * MS: MS09-067
<http://www.microsoft.com/technet/security/Bulletin/MS09-067.mspx>
- * BID: 36908
<http://www.securityfocus.com/bid/36908>
- * VUPEN: VUPEN/ADV-2009-3193
<http://www.vupen.com/english/advisories/2009/3193>
- * SECTRACK: 1023157
<http://securitytracker.com/alerts/2009/Nov/1023157.html>

CVE Reference:

CVE-2009-3131 (cve.mitre.org, nvd.nist.gov)

• 18596 Excel Index Parsing Vulnerability (MS09-067/972652) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Office Excel as a result of pointer corruption when loading Excel formulas. The vulnerability could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed formula. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

- * MS: MS09-067
<http://www.microsoft.com/technet/security/Bulletin/MS09-067.mspx>
- * BID: 36909
<http://www.securityfocus.com/bid/36909>
- * VUPEN: VUPEN/ADV-2009-3193
<http://www.vupen.com/english/advisories/2009/3193>
- * SECTRACK: 1023157
<http://securitytracker.com/alerts/2009/Nov/1023157.html>

CVE Reference:

CVE-2009-3132 (cve.mitre.org, nvd.nist.gov)

• 18597 Excel Document Parsing Memory Corruption Vulnerability (MS09-067/972652) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Office Excel as a result of memory corruption when loading Excel records. The vulnerability could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed object. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

- * MS: MS09-067
<http://www.microsoft.com/technet/security/Bulletin/MS09-067.mspx>
- * BID: 36911
<http://www.securityfocus.com/bid/36911>
- * VUPEN: VUPEN/ADV-2009-3193
<http://www.vupen.com/english/advisories/2009/3193>
- * SECTRACK: 1023157
<http://securitytracker.com/alerts/2009/Nov/1023157.html>

CVE Reference:

CVE-2009-3133 (cve.mitre.org, nvd.nist.gov)

• 18598 Excel Field Sanitization Vulnerability (MS09-067/972652) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Office Excel that could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed record object. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

* MS: MS09-067

<http://www.microsoft.com/technet/security/Bulletin/MS09-067.msp>

* BID: 36912

<http://www.securityfocus.com/bid/36912>

* VUPEN: VUPEN/ADV-2009-3193

<http://www.vupen.com/english/advisories/2009/3193>

* SECTRACK: 1023157

<http://securitytracker.com/alerts/2009/Nov/1023157.html>

CVE Reference:

CVE-2009-3134 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-3135 Microsoft CVSS 2.0 Score = 10.0

Microsoft Office Word 2002 SP3 and 2003 SP3, Office 2004 and 2008 for Mac, Open XML File Format Converter for Mac, Office Word Viewer 2003 SP3, and Office Word Viewer allow remote attackers to execute arbitrary code via a Word document with a malformed record, aka "Microsoft Office Word File Information Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-068.msp>

CVE Reference: [CVE-2009-3135](http://cve.mitre.org/cve/2009/3135)

• CVE-2009-2512 Microsoft CVSS 2.0 Score = 9.3

The Web Services on Devices API (WSDAPI) in Windows Vista Gold, SP1, and SP2 and Server 2008 Gold and SP2 does not properly process the headers of WSD messages, which allows remote attackers to execute arbitrary code via a crafted (1) message or (2) response, aka "Web Services on Devices API Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-063.msp>

CVE Reference: [CVE-2009-2512](http://cve.mitre.org/cve/2009/2512)

• CVE-2009-2514 Microsoft CVSS 2.0 Score = 9.3

win32k.sys in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not correctly parse font code during construction of a directory-entry table, which allows remote attackers to execute arbitrary code via a crafted Embedded OpenType (EOT) font, aka "Win32k EOT Parsing Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-065.msp>

CVE Reference: [CVE-2009-2514](http://cve.mitre.org/cve/2009/2514)

• CVE-2009-2523 Microsoft CVSS 2.0 Score = 9.3

Heap-based buffer overflow in the License Logging Server in Microsoft Windows 2000 SP4 allows remote attackers to execute arbitrary code via an RPC message containing a string with a crafted length, aka "License Logging Server Heap Overflow Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-064.msp>

CVE Reference: [CVE-2009-2523](#)

• **CVE-2009-3127 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office Excel 2002 SP3 and 2003 SP3, Office 2004 and 2008 for Mac, Open XML File Format Converter for Mac, and Office Excel Viewer 2003 SP3 do not properly parse the Excel file format, which allows remote attackers to execute arbitrary code via a crafted spreadsheet, aka "Excel Cache Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-067.msp>

CVE Reference: [CVE-2009-3127](#)

• **CVE-2009-3128 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office Excel 2002 SP3 and 2003 SP3, and Office Excel Viewer 2003 SP3, does not properly parse the Excel file format, which allows remote attackers to execute arbitrary code via a spreadsheet with a malformed record object, aka "Excel SxView Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-067.msp>

CVE Reference: [CVE-2009-3128](#)

• **CVE-2009-3129 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office Excel 2002 SP3, 2003 SP3, and 2007 SP1 and SP2; Office 2004 and 2008 for Mac; Open XML File Format Converter for Mac; Office Excel Viewer 2003 SP3; Office Excel Viewer SP1 and SP2; and Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2 do not properly parse the Excel file format, which allows remote attackers to execute arbitrary code via a spreadsheet with a malformed record object, aka "Excel Featheader Record Memory Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-067.msp>

CVE Reference: [CVE-2009-3129](#)

• **CVE-2009-3130 Microsoft CVSS 2.0 Score = 9.3**

Heap-based buffer overflow in Microsoft Office Excel 2002 SP3, Office 2004 and 2008 for Mac, and Open XML File Format Converter for Mac allows remote attackers to execute arbitrary code via a spreadsheet containing a malformed Binary File Format (aka BIFF) record that triggers memory corruption, aka "Excel Document Parsing Heap Overflow Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-067.msp>

CVE Reference: [CVE-2009-3130](#)

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