

## 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

[Sapphire Worm Scanner](#) - The S4 Sapphire 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 SQL buffer overflow vulnerability (MS02-039/MS02-061) that the recent Sapphire Worm uses to propagate.

Download Here:

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

## This Week in Review

In need of compliance. IT security facing hard times convincing companies to keep up good security. Who's to blame - the QSA or the customer. New UK Political party built on technology reform.

Enjoy reading & Stay safe.

**Call or email netVigilance to get an update on SecureScout.**

**(503) 524 5758 or [sales@netvigilance.com](mailto:sales@netvigilance.com)**

## Top Security News Stories this Week

### • Small businesses largely not PCI compliant

A recent survey has found that a significant portion of small businesses are not compliant with Payment Card Industry Data Security Standard (PCI DSS).

The survey was conducted by compliance vendor ControlScan, the National Retail Federation and the PCI Knowledge Base. Released Monday, it tallied the responses of 220 small businesses, classified as those merchants processing 20,000 or fewer Visa e-commerce transactions each year. It found that though 83 percent of small businesses are familiar with PCI DSS, only 62 percent are compliant.

Some respondents said the standards should be refined so they are more easily understood by less technical retailers. Others said they would like to see the PCI Security Standards Council, which administers the guidelines, offer more help to small businesses. SC Magazine

Full Story :

<http://www.scmagazineus.com/Small-businesses-largely-not-PCI-compliant/article/141557/>

## • **Opinion: Now is the time for IT to update its information security program**

Computerworld - The good news for security teams is that they are more visible to the business than ever before. High-profile data breaches, costly compliance requirements, and a bleak economic market mean companies are more willing to invest in information security to protect their digital assets. But there's bad news, too: Security teams are more visible than ever. With visibility comes an increased set of responsibilities.

Chief information security officers (CISO) have long enjoyed a love-hate relationship with the business. They often serve as strategic counsel and help advise the business on the risks being undertaken. When times are good, companies generally have a stable risk appetite, and CISOs help avoid potential threats to the business. But when times are bad, companies are tempted to change their risk posture in order to enter new markets, reach out to customers through new channels, augment staff, etc. That's when the CISO's job gets tricky. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9136623/Opinion Now is the time for IT to update its information security program](http://www.computerworld.com/s/article/9136623/Opinion_Now_is_the_time_for_IT_to_update_its_information_security_program)

## • **Will the Real Enemy of Security Please Stand Up?**

CSO - A very heated reaction has followed the interview I conducted yesterday with Robert Carr, CEO of Heartland Payment Systems. One reader even said the resulting Q&A made his "blood boil."

Why the outrage? Because Carr did something a lot of people find unacceptable. He threw someone else under the proverbial bus for his company's failure to keep customer credit and debit card numbers out of evil hands. Specifically, he thrust an angry finger at the QSAs who came in to inspect the security controls Heartland had in place to meet the requirements of PCI security. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9136639/Will the Real Enemy of Security Please Stand Up ?source=rss](http://www.computerworld.com/s/article/9136639/Will_the_Real_Enemy_of_Security_Please_Stand_Up_?source=rss)

## • **U.K. gets its own Pirate Party**

The Pirate Party UK, which is dedicated to technology and copyright-law reform, has become an official political party.

The party was registered by the Electoral Commission this week, the party's leader Andrew Robinson told ZDNet UK.

"We're still in the early stages of forming the party," Robinson said Thursday. "We're still very small." Cnet Security

Full Story :

[http://news.cnet.com/8301-1023\\_3-10309960-93.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-1023_3-10309960-93.html?part=rss&subj=news&tag=2547-1_3-0-20)

# **New Vulnerabilities Tested in SecureScout**

## • **13719 Oracle Database Server - Secure Enterprise Search component unspecified Vulnerability (jul-2009/CVE-2009-1968)**

An unspecified vulnerability with unknown impact exists in Oracle Database Server "Secure Enterprise Search" component.

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

### **References:**

\* BUGTRAQ: 20090716 [DSECRG-09-025] Oracle Secure Enterprise Search 10.1.8 Linked XSS vulnerability  
<http://archives.neohapsis.com/archives/bugtraq/2009-07/0110.html>

\* MISC:

<http://dsecrg.com/pages/vul/show.php?id=125>

\* CONFIRM:

<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2009.html>

\* BID: 35681

<http://www.securityfocus.com/bid/35681>

\* OSVDB: 55892

<http://osvdb.org/55892>

\* SECTRACK: 1022560

<http://www.securitytracker.com/id?1022560>

\* SECUNIA: 35776

<http://secunia.com/advisories/35776>

\* VUPEN: ADV-2009-1900

<http://www.vupen.com/english/advisories/2009/1900>

### **CVE Reference:**

CVE-2009-1968 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **13720 Oracle Database Server - Core RDBMS component unspecified Vulnerability (jul-2009/CVE-2009-1015)**

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

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

**References:**

\* CONFIRM:

<http://www.oracle.com/technology/depoy/security/critical-patch-updates/cpujul2009.html>

\* BID: 35682

<http://www.securityfocus.com/bid/35682>

\* OSVDB: 55893

<http://osvdb.org/55893>

\* SECTRAK: 1022560

<http://www.securitytracker.com/id?1022560>

\* SECUNIA: 35776

<http://secunia.com/advisories/35776>

\* VUPEN: ADV-2009-1900

<http://www.vupen.com/english/advisories/2009/1900>

**CVE Reference:**

CVE-2009-1015 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18464 Microsoft Office Web Components Memory Allocation Vulnerability (MS09-043/957638) (Remote File Checking)**

A remote code execution vulnerability exists in the Office Web Components ActiveX Control. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user.

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

**References:**

\* MS: MS09-043

<http://www.microsoft.com/technet/security/bulletin/ms09-043.msp>

\* BID: 35990

<http://www.securityfocus.com/bid/35990>

**CVE Reference:**

CVE-2009-0562 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18465 Microsoft Office Web Components Heap Corruption Vulnerability (MS09-043/957638) (Remote File Checking)**

A remote code execution vulnerability exists in the Office Web Components ActiveX Control. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user.

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

**References:**

\* MS: MS09-043

<http://www.microsoft.com/technet/security/bulletin/ms09-043.msp>

\* BID: 35991

<http://www.securityfocus.com/bid/35991>

**CVE Reference:**

CVE-2009-2496 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18466 Microsoft Office Web Components HTML Script Vulnerability (MS09-043/957638) (Remote File Checking)**

A remote code execution vulnerability exists in the Office Web Components ActiveX Control. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user

rights as the logged-on user.

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

**References:**

\* MS: MS09-043

<http://www.microsoft.com/technet/security/bulletin/ms09-043.msp>

\* BID: 35642

<http://www.securityfocus.com/bid/35642/>

**CVE Reference:**

CVE-2009-1136 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **18467 Microsoft Office Web Components Buffer Overflow Vulnerability (MS09-043/957638) (Remote File Checking)**

A remote code execution vulnerability exists in the Office Web Components ActiveX Control. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user.

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

**References:**

\* MS: MS09-043

<http://www.microsoft.com/technet/security/bulletin/ms09-043.msp>

\* BID: 35992

<http://www.securityfocus.com/bid/35992>

**CVE Reference:**

CVE-2009-1534 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **18468 Remote Desktop Connection Heap Overflow Vulnerability (MS09-044/970927) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Remote Desktop Connection (formerly known as Terminal Services Client) processes specific parameters returned by the RDP server. An attacker who successfully exploited this vulnerability could take complete control of an affected system remotely. An attacker could then install programs or 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: MS09-044

<http://www.microsoft.com/technet/security/bulletin/ms09-044.msp>

\* BID: 35971

<http://www.securityfocus.com/bid/35971>

**CVE Reference:**

CVE-2009-1133 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **18469 Remote Desktop Connection ActiveX Control Heap Overflow Vulnerability (MS09-044/970927) (Remote File Checking)**

A remote code execution vulnerability exists in the Microsoft Terminal Services Client ActiveX control. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially allow remote code execution if a user visited that page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

**References:**

\* MS: MS09-044

<http://www.microsoft.com/technet/security/bulletin/ms09-044.msp>

\* BID: 35973

<http://www.securityfocus.com/bid/35973>

**CVE Reference:**

CVE-2009-1929 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • **18470 WINS Heap Overflow Vulnerability (MS09-039/969883) (Remote File Checking)**

A remote code execution vulnerability exists in the Windows Internet Name Service (WINS) due to a buffer overflow caused by incorrect calculation of buffer length when processing specially crafted WINS network packets. 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.

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

#### References:

\* MS: MS09-039

<http://www.microsoft.com/technet/security/bulletin/ms09-039.msp>

\* BID: 35980

<http://www.securityfocus.com/bid/35980>

#### CVE Reference:

CVE-2009-1923 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • **18471 WINS Integer Overflow Vulnerability (MS09-039/969883) (Remote File Checking)**

A remote code execution vulnerability exists in the default configuration of the Windows Internet Name Service (WINS) due to insufficient validation of data structures within specially crafted WINS network packets received from a trusted WINS replication partner.

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

#### References:

\* MS: MS09-039

<http://www.microsoft.com/technet/security/bulletin/ms09-039.msp>

\* BID: 35981

<http://www.securityfocus.com/bid/35981>

#### CVE Reference:

CVE-2009-1924 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

### • **CVE-2009-1133 Microsoft CVSS 2.0 Score = 10.0**

Heap-based buffer overflow in Microsoft Remote Desktop Connection (formerly Terminal Services Client) running RDP 5.0 through 6.1 on Windows, and Remote Desktop Connection Client for Mac 2.0, allows remote attackers to execute arbitrary code via unspecified parameters, aka "Remote Desktop Connection Heap Overflow Vulnerability."

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

#### References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-044.msp>

CVE Reference: [CVE-2009-1133](http://cve.mitre.org)

### • **CVE-2009-1545 Microsoft CVSS 2.0 Score = 10.0**

Unspecified vulnerability in the Windows Media file handling functionality in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a malformed header in a crafted AVI file, aka "Malformed AVI Header Vulnerability."

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

#### References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-038.msp>

CVE Reference: [CVE-2009-1545](http://cve.mitre.org)

### • **CVE-2009-1546 Microsoft CVSS 2.0 Score = 10.0**

Integer overflow in the Windows Media file handling functionality in Microsoft Windows allows remote attackers to execute arbitrary code on a Windows 2000 SP4 system via a crafted AVI file, or cause a denial of service on a Windows XP SP2 or SP3, Server 2003 SP2, Vista Gold, SP1, or SP2, or Server 2008 Gold or SP2 system via a crafted AVI file, aka "AVI Integer Overflow Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-038.msp>

**CVE Reference:** [CVE-2009-1546](#)

• **CVE-2009-1930 Microsoft CVSS 2.0 Score = 10.0**

The Telnet service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote Telnet servers to execute arbitrary code on a client machine by replaying the NTLM credentials of a client user, aka "Telnet Credential Reflection Vulnerability," a related issue to CVE-2000-0834.

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

**References:**

VUPEN: <http://www.vupen.com/english/advisories/2009/2237>

BID: <http://www.securityfocus.com/bid/35993>

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-042.msp>

SECTRAK: <http://securitytracker.com/id?1022716>

SECUNIA: <http://secunia.com/advisories/36222>

**CVE Reference:** [CVE-2009-1930](#)

• **CVE-2009-2494 Microsoft CVSS 2.0 Score = 10.0**

The Active Template Library (ATL) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via vectors related to erroneous free operations after reading a variant from a stream and deleting this variant, aka "ATL Object Type Mismatch Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-037.msp>

**CVE Reference:** [CVE-2009-2494](#)

• **CVE-2009-0562 Microsoft CVSS 2.0 Score = 9.3**

The Office Web Components ActiveX Control in Microsoft Office XP SP3, Office 2003 SP3, Office XP Web Components SP3, Office 2003 Web Components SP3, Office 2003 Web Components SP1 for the 2007 Microsoft Office System, Internet Security and Acceleration (ISA) Server 2004 SP3 and 2006 SP1, and Office Small Business Accounting 2006 does not properly allocate memory, which allows remote attackers to execute arbitrary code via unspecified vectors that trigger "system state" corruption, aka "Office Web Components Memory Allocation Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-043.msp>

**CVE Reference:** [CVE-2009-0562](#)

• **CVE-2009-1534 Microsoft CVSS 2.0 Score = 9.3**

Buffer overflow in the Office Web Components ActiveX Control in Microsoft Office XP SP3, Office 2000 Web Components SP3, Office XP Web Components SP3, BizTalk Server 2002, and Visual Studio .NET 2003 SP1 allows remote attackers to execute arbitrary code via crafted property values, aka "Office Web Components Buffer Overflow Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-043.msp>

**CVE Reference:** [CVE-2009-1534](#)

• **CVE-2009-1923 Microsoft CVSS 2.0 Score = 9.3**

Heap-based buffer overflow in the Windows Internet Name Service (WINS) component for Microsoft Windows 2000 SP4 and Server 2003 SP2 allows remote attackers to execute arbitrary code via a crafted WINS replication packet that triggers an incorrect buffer-length calculation, aka "WINS Heap Overflow Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-039.mspx>

**CVE Reference:** [CVE-2009-1923](#)

**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](mailto: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](mailto: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](mailto:info-scanner@securescout.net)