

## 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

[WinHoneyd v1.5b](#) - Download WinHoneyd executable package by filling our download form. Size: 2404KB

Download Here:

<http://www.netvigilance.com/productdownloads?productname=winhoneyd-1.5b.zip>

## This Week in Review

One of the original designers speak of what the internet is lacking. Data loss top concern. How to decide on web app firewall. A story from 'real life' security.

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

### • The Internet is incomplete, says its co-designer, Vinton Cerf

Computerworld - WASHINGTON - The co-designer of the Internet's basic architecture, Vinton Cerf, said the Internet "still lacks many of the features that it needs," particularly in security, during a blunt talk to a tech industry crowd here.

Cerf is influential because of his accomplishments, but he may be even more so today because of his affiliation with Google. President Obama's administration has appointed a number of Google employees, including CEO Eric Schmidt, to important positions.

The lack of authentication is pervasive and is even a problem in simple cases, such as authenticating entries in the domain name system, he said.

Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9134246>

### • Data loss is the top concern in the enterprise

Security professionals are well aware of the dangers to a company's bottom line caused by the loss of a laptop, smart phone or other mobile device. What corporate secrets are now available to intruders? How will the leakage of corporate assets or confidential customer data affect the company's reputation, nevermind the costs incurred from meeting regulatory demands committing the organization to contact everyone affected.

Persuading those in control of the corporate purse strings of the necessity of having tools and strategies in place to guard against such a scenario is no easy task, particularly in these slow economic times when budget dollars are hard to come by.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Data-loss-is-the-top-concern-in-the-enterprise/article/138376/>

### • Web App Firewalls: How to Evaluate, Buy, Implement

CSO - A Web application firewall (WAF) is designed to protect Web applications against common attacks such as cross-site scripting and SQL injection. Whereas network firewalls defend the perimeter of the network, WAFs sit between the Web client and Web server, analyzing application-layer traffic for violations in the programmed security policy, says Michael Cobb, founder of Cobweb Applications, a security consultancy.

WAFs also differ from intrusion prevention systems. "It's a very different technology--it's not signature-based, it's behavioral, and it protects against vulnerabilities you [inadvertently] create yourself," says Greg Young, an analyst at Gartner.

Main WAF Attributes

Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9134228>

### • Undercover: A Case of Help Desk Failure

CSO - As the engagement leader on security assessment projects for our clients, I frequently run into what I call the "IT Myopathy Syndrome."

Here's an example of one such case.

Once we sat down, plugged in our computers (to check e-mail, of course) and started feeling a bit more comfortable, the director of IT security walked into the room and started a conversation with us.

Computerworld

Full Story :

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9134245>

## New Vulnerabilities Tested in SecureScout

### • 18405 Internet Explorer Race Condition Cross-Domain Information Disclosure Vulnerability (MS09-019/969897) (Remote File Checking)

An information disclosure vulnerability exists in Internet Explorer that could allow script to gain access to the content in another browser window in another domain or Internet Explorer zone. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow information disclosure if a user viewed the Web page. An attacker who successfully exploited this vulnerability could view data from a Web page in another Internet Explorer domain.

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

#### References:

- \* BUGTRAQ: 20070604 Assorted browser vulnerabilities  
<http://www.securityfocus.com/archive/1/archive/1/470446/100/0/threaded>
- \* FULLDISC: 20070604 Assorted browser vulnerabilities  
<http://archives.neohapsis.com/archives/fulldisclosure/2007-06/0026.html>
- \* MISC:  
<http://lcamtuf.coredump.cx/ierace/>
- \* CERT-VN: VU#471361  
<http://www.kb.cert.org/vuls/id/471361>

\* BID: 24283  
<http://www.securityfocus.com/bid/24283>  
\* VUPEN: ADV-2007-2064  
<http://www.frsirt.com/english/advisories/2007/2064>  
\* SECTRACK: 1018192  
<http://securitytracker.com/id?1018192>  
\* SECUNIA: 25564  
<http://secunia.com/advisories/25564>  
\* SREASON: 2781  
<http://securityreason.com/securityalert/2781>  
\* XF: ie-pageupdate-security-bypass(34696)  
<http://xforce.iss.net/xforce/xfdb/34696>

**CVE Reference:**

CVE-2007-3091 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **18406 Internet Explorer Cross-Domain Information Disclosure Vulnerability (MS09-019/969897) (Remote File Checking)**

An information disclosure vulnerability exists in the way that Internet Explorer caches data and incorrectly allows the cached content to be called, potentially bypassing Internet Explorer domain restriction. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow information disclosure if a user viewed the Web page. An attacker who successfully exploited this vulnerability could view content from the local computer or another browser window in another domain or Internet Explorer zone.

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

**References:**

\* MS: MS09-019  
<http://www.microsoft.com/technet/security/Bulletin/MS09-019.msp>  
\* BID: 35200  
<http://www.securityfocus.com/bid/35200>

**CVE Reference:**

CVE-2009-1140 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **18407 Internet Explorer DHTML Object Memory Corruption Vulnerability (MS09-019/969897) (Remote File Checking)**

A remote code execution vulnerability exists in the way Internet Explorer displays a Web page that contains certain unexpected method calls to HTML objects. As a result, system memory may be corrupted in such a way that an attacker could execute arbitrary code if a user visited a specially crafted Web site. 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: MS09-019  
<http://www.microsoft.com/technet/security/Bulletin/MS09-019.msp>  
\* BID: 35198  
<http://www.securityfocus.com/bid/35198>

**CVE Reference:**

CVE-2009-1141 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **18408 Internet Explorer HTML Object Memory Corruption Vulnerability (CVE-2009-1528) (MS09-019/969897) (Remote File Checking)**

A remote code execution vulnerability exists in the way Internet Explorer accesses an object that has not been correctly initialized or has been deleted. 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. If a user is logged on with administrative user rights, 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: MS09-019

<http://www.microsoft.com/technet/security/Bulletin/MS09-019.msp>

\* BID: 35222

<http://www.securityfocus.com/bid/35222>

**CVE Reference:**

CVE-2009-1528 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18409 Internet Explorer Uninitialized Memory Corruption Vulnerability (MS09-019/969897) (Remote File Checking)**

A remote code execution vulnerability exists in the way Internet Explorer accesses an object that has not been correctly initialized or has been deleted. 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. If a user is logged on with administrative user rights, 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: MS09-019

<http://www.microsoft.com/technet/security/Bulletin/MS09-019.msp>

\* BID: 35223

<http://www.securityfocus.com/bid/35223>

**CVE Reference:**

CVE-2009-1529 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18410 Internet Explorer HTML Objects Memory Corruption Vulnerability (MS09-019/969897) (Remote File Checking)**

A remote code execution vulnerability exists in the way Internet Explorer accesses an object that has not been correctly initialized or has been deleted. 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. If a user is logged on with administrative user rights, 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: MS09-019

<http://www.microsoft.com/technet/security/Bulletin/MS09-019.msp>

\* BID: 35224

<http://www.securityfocus.com/bid/35224>

**CVE Reference:**

CVE-2009-1530 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18411 Internet Explorer HTML Object Memory Corruption Vulnerability (CVE-2009-1531) (MS09-019/969897) (Remote File Checking)**

A remote code execution vulnerability exists in the way Internet Explorer accesses an object that has not been correctly initialized or has been deleted. 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. If a user is logged on with administrative user rights, 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: MS09-019

<http://www.microsoft.com/technet/security/Bulletin/MS09-019.msp>

\* BID: 35234

<http://www.securityfocus.com/bid/35234>

**CVE Reference:**

CVE-2009-1531 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18412 Internet Explorer HTML Object Memory Corruption Vulnerability (CVE-2009-1532) (MS09-019/969897) (Remote File Checking)**

A remote code execution vulnerability exists in the way Internet Explorer accesses an object that has not been correctly initialized or has been deleted. 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. If a user is logged on with administrative user rights, 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: MS09-019

<http://www.microsoft.com/technet/security/Bulletin/MS09-019.msp>

\* BID: 35235

<http://www.securityfocus.com/bid/35235>

**CVE Reference:**

CVE-2009-1532 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18413 Active Directory Invalid Free Vulnerability (MS09-018/971055) (Remote File Checking)**

A remote code execution vulnerability exists in implementations of Active Directory on Microsoft Windows 2000 Server. The vulnerability is due to incorrect freeing of memory when processing specially crafted LDAP or LDAPS requests. 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: MS09-018

<http://www.microsoft.com/technet/security/Bulletin/MS09-018.msp>

\* BID: 35226

<http://www.securityfocus.com/bid/35226>

**CVE Reference:**

CVE-2009-1138 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **18414 Active Directory Memory Leak Vulnerability (MS09-018/971055) (Remote File Checking)**

A denial of service vulnerability exists in implementations of Active Directory on Microsoft Windows 2000 Server and Windows Server 2003. The vulnerability also exists in implementations of Active Directory Application Mode (ADAM) when installed on Windows XP Professional and Windows Server 2003. The vulnerability is due to improper memory management during execution of certain types of LDAP or LDAPS requests. An attacker who successfully exploited this vulnerability could cause the affected server to stop responding.

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

**References:**

\* MS: MS09-018

<http://www.microsoft.com/technet/security/Bulletin/MS09-018.msp>

\* BID: 35225

<http://www.securityfocus.com/bid/35225>

**CVE Reference:**

CVE-2009-1139 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

- **CVE-2009-0228 Microsoft CVSS 2.0 Score = 10.0**

Buffer overflow in the Windows Print Spooler in Microsoft Windows 2000 SP4 allows remote attackers to execute arbitrary code via a crafted RPC request in conjunction with availability of a print server with a crafted ShareName, related to "printing data structures," aka "Buffer Overflow in Print Spooler Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-022.msp>

**CVE Reference:** [CVE-2009-0228](#)

• **CVE-2009-1138 Microsoft CVSS 2.0 Score = 10.0**

The LDAP service in Active Directory on Microsoft Windows 2000 SP4 does not properly free memory for LDAP and LDAPS requests, which allows remote attackers to execute arbitrary code via a crafted request packet, aka "Active Directory Invalid Free Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-018.msp>

**CVE Reference:** [CVE-2009-1138](#)

• **CVE-2009-0563 Microsoft CVSS 2.0 Score = 9.3**

Buffer overflow in Microsoft Office Word 2002 SP3, 2003 SP3, and 2007 SP1 and SP2; Microsoft Office for Mac 2004 and 2008; Open XML File Format Converter for Mac; Microsoft Office Word Viewer 2003 SP3; Microsoft Office Word Viewer; and Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2 allows remote attackers to execute arbitrary code via a Word document with a malformed record that triggers memory corruption, aka "Word Buffer Overflow Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-027.msp>

**CVE Reference:** [CVE-2009-0563](#)

• **CVE-2009-0565 Microsoft CVSS 2.0 Score = 9.3**

Buffer overflow in Microsoft Office Word 2000 SP3, 2002 SP3, and 2007 SP1 and SP2; Microsoft Office for Mac 2004 and 2008; Open XML File Format Converter for Mac; and Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2 allows remote attackers to execute arbitrary code via a Word document with a malformed record that triggers memory corruption, aka "Word Buffer Overflow Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-027.msp>

**CVE Reference:** [CVE-2009-0565](#)

• **CVE-2009-0568 Microsoft CVSS 2.0 Score = 9.3**

The RPC Marshalling Engine (aka NDR) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 SP2 does not properly maintain its internal state, which allows remote attackers to overwrite arbitrary memory locations via a crafted RPC message that triggers incorrect pointer reading, related to "IDL interfaces containing a non-conformant varying array" and FC\_SMVARRAY, FC\_LGVARRAY, FC\_VARIABLE\_REPEAT, and FC\_VARIABLE\_OFFSET, aka "RPC Marshalling Engine Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-026.msp>

**CVE Reference:** [CVE-2009-0568](#)

• **CVE-2009-1533 Microsoft CVSS 2.0 Score = 9.3**

Buffer overflow in the Works for Windows document converters in Microsoft Office 2000 SP3, Office XP SP3, Office 2003 SP3, Office 2007 SP1, and Works 8.5 and 9 allows remote attackers to execute arbitrary code via a crafted Works .wps file that triggers memory corruption, aka "File Converter Buffer Overflow Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-024.msp>

**CVE Reference:** [CVE-2009-1533](#)

• **CVE-2009-0549 Microsoft CVSS 2.0 Score = 9.3**

Excel in Microsoft Office 2000 SP3, Office XP SP3, Office 2003 SP3, and Office 2004 and 2008 for Mac; Open XML File Format Converter for Mac; and Microsoft Office Excel Viewer 2003 SP3 allow remote attackers to execute arbitrary code via a crafted Excel file with a malformed record object, aka "Record Pointer Corruption Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-021.msp>

**CVE Reference:** [CVE-2009-0549](#)

• **CVE-2009-0557 Microsoft CVSS 2.0 Score = 9.3**

Excel in Microsoft Office 2000 SP3, Office XP SP3, Office 2003 SP3, and Office 2004 and 2008 for Mac; Excel in 2007 Microsoft Office System SP1 and SP2; Open XML File Format Converter for Mac; Microsoft Office Excel Viewer 2003 SP3; Microsoft Office Excel Viewer; and Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2 allow remote attackers to execute arbitrary code via a crafted Excel file with a malformed record object, aka "Object Record Corruption Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-021.msp>

**CVE Reference:** [CVE-2009-0557](#)

**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)