

## 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

[Apache Chunked Vulnerability Scanner](#) - The S4 Apache Chunked Vulnerability 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 Apache Chunked Encoding buffer overflow.

Download Here:

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

## This Week in Review

The first 2011 predictions are here. A number of websites affected by breach. OpenBSD and FBI. A pessimistic look at the future.

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

### • More censorship, data breaches and devices: Security predictions for 2011

Network World - This past year has been a doozy in the security world. We kicked off the year by discovering operation Aurora, saw the first national-industrial sabotage attack with Stuxnet and are closing the year with Wikileaks about to become a constitutional crisis between the First amendment and a 1917 espionage law. Reality has well and truly become weirder than fiction.

Let me dive in and make some predictions for security in 2011:

Also read: What would your ultimate network security look like? Computerworld

Full Story :

[http://www.computerworld.com/s/article/9201418/More\\_censorship\\_data\\_breaches\\_and\\_devices\\_Security\\_prediction](http://www.computerworld.com/s/article/9201418/More_censorship_data_breaches_and_devices_Security_prediction)

### • Gawker breach prompts LinkedIn, Yahoo password resets

The recent theft of approximately 1.3 million account details from the servers of online media company Gawker has prompted password resets at a number of popular websites, including Yahoo, LinkedIn and Blizzard Entertainment's World of Warcraft.

Social media site LinkedIn said it has identified a "very small fraction" of its members whose accounts could potentially be affected by the breach.

"As we closely monitored the situation, we decided it was imperative to take pre-emptive action to help ensure that those leaked passwords were not being used to attack any LinkedIn members," Vincente Silveira, principal product manager at LinkedIn, wrote in a blog post Tuesday. SC Magazine

Full Story :

[http://www.scmagazineus.com/gawker-breach-prompts-linkedin-yahoo-password-resets/article/192946/?utm\\_source](http://www.scmagazineus.com/gawker-breach-prompts-linkedin-yahoo-password-resets/article/192946/?utm_source)

#### • **Report of FBI back door roils OpenBSD community**

Allegations that the FBI surreptitiously placed a back door into the OpenBSD operating system have alarmed the computer security community, prompting calls for an audit of the source code and claims that the charges must be a hoax.

The report surfaced in e-mail made public yesterday from a former government contractor, who alleged that he worked with the FBI to implement "a number of back doors" in OpenBSD, which has a reputation for high security and is used in some commercial products.

Gregory Perry, the former chief technologist at the now-defunct contractor Network Security Technology, or NETSEC, said he's disclosing this information now because his 10-year confidentiality agreement with the FBI has expired. The e-mail was sent to OpenBSD founder Theo de Raadt, who posted it publicly. Cnet Security

Full Story :

[http://news.cnet.com/8301-31921\\_3-20025767-281.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-31921_3-20025767-281.html?part=rss&subj=news&tag=2547-1_3-0-20)

#### • **Goodbye Internet, we hardly knew ye?**

Network World - This end-of-year article is a looking forward one -- looking forward to a year in which the Internet will be under a multi-pronged attack that threatens to change it irrevocably in ways that may destroy much of the Internet's potential.

Also read: 2010's biggest security snafus

Throughout its history, the Internet, in most places, has been essentially free from government regulation. There are significant exceptions -- a few countries do quite an effective job of controlling Internet content and a number of countries control specific Internet technologies such as encryption and VoIP. But, on the whole, the Internet has been left alone to disrupt businesses, governments and society. The Internet's impact on the music and film businesses, newspapers, privacy, social unrest, government transparency (voluntary and otherwise), and education, among many other things, has been profound. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9201080/Goodbye\\_Internet\\_we\\_hardly\\_knew\\_ye?source=rss\\_security](http://www.computerworld.com/s/article/9201080/Goodbye_Internet_we_hardly_knew_ye?source=rss_security)

## **New Vulnerabilities Tested in SecureScout**

#### • **13605 IPsec VPN detected (IKE)**

The remote host is enabled to do Internet Key Exchange (IKE). This is typically indicative of a VPN server. VPN servers allow to connect remote hosts into internal resources.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Low**

References:

\* MISC:

<http://www.nta-monitor.com/posts/2005/01/VPN-Flaws-Whitepaper.pdf>

CVE Reference:

#### • **19091 Windows MFC Document Title Updating Buffer Overflow Vulnerability (MS10-074/2387149) (Remote File Checking)**

A remote code execution vulnerability exists in the way that window titles are managed in applications written using the Microsoft Foundation Class (MFC) Library. While the vulnerability is located in MFC and is present on affected operating systems, it can only be exploited if a remote attacker can influence the window title of any window in an

MFC application. An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the current user.

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

#### References:

- \* VUPEN: VUPEN/ADV-2010-2621  
<http://www.vupen.com/english/advisories/2010/2621>
- \* BID: 41333  
<http://www.securityfocus.com/bid/41333>
- \* SECTRACK: 1024705  
<http://securitytracker.com/alerts/2010/Nov/1024705.html>
- \* NETVIGILANCE-UNKNOWN: 13921  
<http://www.exploit-db.com/exploits/13921/>
- \* MISC:  
[http://www.eeye.com/Resources/Security-Center/Research/Zero-Day-Tracker/2010/20100705-\(1\)](http://www.eeye.com/Resources/Security-Center/Research/Zero-Day-Tracker/2010/20100705-(1))
- \* MS: MS10-074  
<http://www.microsoft.com/technet/security/Bulletin/MS10-074.mspx>
- \* SECTRACK: 1024557  
<http://securitytracker.com/id?1024557>

#### CVE Reference:

CVE-2010-3227 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19096 TLSv1 Denial of Service Vulnerability (MS10-085/2207566) (Remote File Checking)

A denial of service vulnerability exists in the way that SChannel processes protocol requests while handling incoming SSL connections on Windows Server 2008, Windows Vista, Windows Server 2008 R2, and Windows 7. A remote, anonymous attacker could send a specially crafted network packet to the affected system that would cause the LSASS service to stop responding and the system to restart. Systems are only affected if a service or application is configured to receive SSL network traffic.

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

#### References:

- \* VUPEN: VUPEN/ADV-2010-2632  
<http://www.vupen.com/english/advisories/2010/2632>
- \* BID: 43780  
<http://www.securityfocus.com/bid/43780>
- \* SECTRACK: 1024556  
<http://securitytracker.com/id?1024556>
- \* CONFIRM:  
<http://support.avaya.com/css/P8/documents/100113338>
- \* MS: MS10-085  
<http://www.microsoft.com/technet/security/Bulletin/MS10-085.mspx>

#### CVE Reference:

CVE-2010-3229 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 19097 HTML Object Memory Corruption Vulnerability (CVE-2010-3340) (MS10-090/2416400) (Remote File Checking)

A remote code execution vulnerability exists in the way that 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:

- \* VUPEN: VUPEN/ADV-2010-3214  
<http://www.vupen.com/english/advisories/2010/3214>
- \* BID: 45255  
<http://www.securityfocus.com/bid/45255>
- \* MS: MS10-090  
<http://www.microsoft.com/technet/security/bulletin/MS10-090.mspx>

**CVE Reference:**

CVE-2010-3340 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

**• 19098 Cross-Domain Information Disclosure Vulnerability (CVE-2010-3342) (MS10-090/2416400) (Remote File Checking)**

An information disclosure vulnerability exists in Internet Explorer that could allow script to gain access to information 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 content from another domain or Internet Explorer zone.

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

**References:**

\* VUPEN: VUPEN/ADV-2010-3214

<http://www.vupen.com/english/advisories/2010/3214>

\* BID: 45256

<http://www.securityfocus.com/bid/45256>

\* MS: MS10-090

<http://www.microsoft.com/technet/security/bulletin/MS10-090.aspx>

**CVE Reference:**

CVE-2010-3342 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

**• 19099 HTML Object Memory Corruption Vulnerability (CVE-2010-3343) (MS10-090/2416400) (Remote File Checking)**

A remote code execution vulnerability exists in the way that 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:**

\* VUPEN: VUPEN/ADV-2010-3214

<http://www.vupen.com/english/advisories/2010/3214>

\* BID: 45259

<http://www.securityfocus.com/bid/45259>

\* MS: MS10-090

<http://www.microsoft.com/technet/security/bulletin/MS10-090.aspx>

**CVE Reference:**

CVE-2010-3343 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

**• 19100 HTML Element Memory Corruption Vulnerability (CVE-2010-3345) (MS10-090/2416400) (Remote File Checking)**

A remote code execution vulnerability exists in the way that 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:**

\* VUPEN: VUPEN/ADV-2010-3214

<http://www.vupen.com/english/advisories/2010/3214>

\* BID: 45260

<http://www.securityfocus.com/bid/45260>

\* MS: MS10-090

<http://www.microsoft.com/technet/security/bulletin/MS10-090.aspx>

**CVE Reference:**

CVE-2010-3345 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

**• 19101 HTML Element Memory Corruption Vulnerability (CVE-2010-3346) (MS10-090/2416400) (Remote File Checking)**

A remote code execution vulnerability exists in the way that 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:**

\* VUPEN: VUPEN/ADV-2010-3214

<http://www.vupen.com/english/advisories/2010/3214>

\* BID: 45261

<http://www.securityfocus.com/bid/45261>

\* MS: MS10-090

<http://www.microsoft.com/technet/security/bulletin/MS10-090.aspx>

**CVE Reference:**

CVE-2010-3346 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

**• 19102 Cross-Domain Information Disclosure Vulnerability (CVE-2010-3348) (MS10-090/2416400) (Remote File Checking)**

An information disclosure vulnerability exists in Internet Explorer that could allow script to gain access to information 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 content from another domain or Internet Explorer zone.

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

**References:**

\* VUPEN: VUPEN/ADV-2010-3214

<http://www.vupen.com/english/advisories/2010/3214>

\* BID: 45263

<http://www.securityfocus.com/bid/45263>

\* MS: MS10-090

<http://www.microsoft.com/technet/security/bulletin/MS10-090.aspx>

**CVE Reference:**

CVE-2010-3348 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

**• 19103 Uninitialized Memory Corruption Vulnerability (MS10-090/2416400) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by convincing the user to open a malicious Word document. When a user closes the document, 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:**

\* VUPEN: VUPEN/ADV-2010-3214

<http://www.vupen.com/english/advisories/2010/3214>

\* BID: 44536

<http://www.securityfocus.com/bid/44536>

\* MS: MS10-090

<http://www.microsoft.com/technet/security/bulletin/MS10-090.aspx>

**CVE Reference:**

## New Vulnerabilities found this Week

- **CVE-2010-2571 Microsoft CVSS 2.0 Score = 9.3**

Array index error in pubconv.dll (aka the Publisher Converter DLL) in Microsoft Publisher 2002 SP3 and 2003 SP3 allows remote attackers to execute arbitrary code via a crafted Publisher 97 file, aka "Memory Corruption Due To Invalid Index Into Array in Pubconv.dll Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-103.msp>

**CVE Reference:** [CVE-2010-2571](#)

- **CVE-2010-2569 Microsoft CVSS 2.0 Score = 9.3**

pubconv.dll (aka the Publisher Converter DLL) in Microsoft Publisher 2002 SP3, 2003 SP3, and 2007 SP2 does not properly handle an unspecified size field in certain older file formats, which allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via a crafted Publisher file, aka "Size Value Heap Corruption in pubconv.dll Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-103.msp>

**CVE Reference:** [CVE-2010-2569](#)

- **CVE-2010-3340 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 6 and 7 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "HTML Object Memory Corruption Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-090.msp>

**CVE Reference:** [CVE-2010-3340](#)

- **CVE-2010-3343 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 6 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "HTML Object Memory Corruption Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-090.msp>

**CVE Reference:** [CVE-2010-3343](#)

- **CVE-2010-3345 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "HTML Element Memory Corruption Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-090.msp>

**CVE Reference:** [CVE-2010-3345](#)

- **CVE-2010-3346 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Internet Explorer 6, 7, and 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing an object that (1) was not properly initialized or (2) is deleted, leading to memory corruption, aka "HTML Element Memory Corruption Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-090.msp>

**CVE Reference:** [CVE-2010-3346](#)

• **CVE-2010-3338 Microsoft CVSS 2.0 Score = 7.2**

The Windows Task Scheduler in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly determine the security context of scheduled tasks, which allows local users to gain privileges via a crafted application, aka "Task Scheduler Vulnerability." NOTE: this might overlap CVE-2010-3888.

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-092.msp>

**CVE Reference:** [CVE-2010-3338](#)

• **CVE-2010-3939 Microsoft CVSS 2.0 Score = 7.2**

Buffer overflow in win32k.sys in the kernel-mode drivers in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows local users to gain privileges via vectors related to improper memory allocation for copies from user mode, aka "Win32k Buffer Overflow Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-098.msp>

**CVE Reference:** [CVE-2010-3939](#)

**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)