

## 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

\$265 million in reported losses last year. Virtualized systems to become most secure. Rogue ISP down for now. Questions organizations need to ask vendors.

netVigilance today issued an urgent bulletin warning all merchants and retailers subject to PCI-DSS Compliance that new PCI regulations significantly increase their chances of PCI failure. To read the bulletin, [click here](#)

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

### • Web fraud losses more than double in 2009, says report

Losses related to cybercrime more than doubled from 2008 to last year, according to a report from the Internet Crime Complaint Center (IC3)

The organization, a partnership between the National White Collar Crime Center and the FBI, received 336,655 complaints with a reported \$559.7 million in losses. In 2008, IC3 received 275,284 reports with \$265 million in reported losses.

Hoax emails claiming to be from the FBI, but which actually were created to steal personal information from the recipient, represented 16.6 percent of all complaints submitted. The next most common complaints were undelivered merchandise, followed by advance-fee schemes, identity theft and overpayment fraud. SC Magazine

Full Story :

[http://www.scmagazineus.com/web-fraud-losses-more-than-double-in-2009-says-report/article/165824/?utm\\_source=](http://www.scmagazineus.com/web-fraud-losses-more-than-double-in-2009-says-report/article/165824/?utm_source=)

### • **Gartner: Virtualization security will take time**

In five years, virtualized systems likely will be more secure than their physical counterparts, but until then, it will be rough sledding for organizations transitioning to the new technology, according to a new report from Gartner.

Through 2012, 60 percent of virtualized servers will be less secure than the physical servers they replace, revealed the findings, released Monday. The analyst firm blamed the stumbling on organizations' failure to involve the IT security team in its deployment projects, in addition to immature tools to protect these new environments. SC Magazine

Full Story :

[http://www.scmagazineus.com/gartner-virtualization-security-will-take-time/article/165932/?utm\\_source=feedburner&](http://www.scmagazineus.com/gartner-virtualization-security-will-take-time/article/165932/?utm_source=feedburner&)

### • **After weeklong fight, rogue ISP Troyak struggles for life**

IDG News Service - After an international take-down effort, a rogue ISP responsible for controlling large numbers of computers infected with data-stealing code is down for the moment, but it may be reconnecting with the Internet, according to security researchers.

Troyak, which is believed to be based in eastern Europe, was knocked offline earlier this month after other networks supplying its connectivity to the Internet stopped carrying its traffic due to complaints it was complicit in cybercrime.

Since then the network has fought a cat-and-mouse game with network providers in 12 countries and international law enforcement, according to Jart Armin, the pseudonymous editor of the Hostexploit.com Web site, which has been involved in the action. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9172198/After\\_weeklong\\_fight\\_rogue\\_ISP\\_Troyak\\_struggles\\_for\\_life?source=](http://www.computerworld.com/s/article/9172198/After_weeklong_fight_rogue_ISP_Troyak_struggles_for_life?source=)

### • **Security group preps IT shops to ask vendors 'nasty questions'**

Network World - The Jericho Forum, which advocates improving e-commerce security through knowledge that network perimeters are fading, says organizations need to ask themselves and their vendors tougher questions.

To assist, the 60-member forum Monday issued its "Self Assessment Scheme".

"We took our best practices and turned them into generic examples," says Paul Simmonds, CISO at pharmaceutical firm AstraZeneca, a Jericho Forum member. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9170738/Security\\_group\\_preps\\_IT\\_shops\\_to\\_ask\\_vendors\\_nasty\\_questions](http://www.computerworld.com/s/article/9170738/Security_group_preps_IT_shops_to_ask_vendors_nasty_questions)

## **New Vulnerabilities Tested in SecureScout**

### • **14553 Adobe Acrobat / Reader buffer overflow Vulnerability (CVE-2009-2994) (Remote File Checking)**

Buffer overflow in Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 might allow attackers to execute arbitrary code via unspecified vectors.

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

#### **References:**

\* CONFIRM:

<http://www.adobe.com/support/security/bulletins/apsb09-15.html>

\* CERT: TA09-286B

<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>

\* BID: 36638

<http://www.securityfocus.com/bid/36638>

\* SECTRACK: 1023007

<http://securitytracker.com/id?1023007>

\* VUPEN: ADV-2009-2898

<http://www.vupen.com/english/advisories/2009/2898>

#### **CVE Reference:**

CVE-2009-2994 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **14554 Adobe Acrobat integer overflow Vulnerability (CVE-2009-2995) (Remote File Checking)**

Integer overflow in Adobe Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 allows attackers to cause a denial of service via unspecified vectors.

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

**References:**

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- \* CERT: TA09-286B  
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- \* BID: 36638  
<http://www.securityfocus.com/bid/36638>
- \* SECTRACK: 1023007  
<http://securitytracker.com/id?1023007>
- \* VUPEN: ADV-2009-2898  
<http://www.vupen.com/english/advisories/2009/2898>

**CVE Reference:**

CVE-2009-2995 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **14555 Adobe Acrobat / Reader memory corruption Vulnerability (CVE-2009-2996) (Remote File Checking)**

Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 allow attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-2985.

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

**References:**

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- \* CERT: TA09-286B  
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- \* BID: 36638  
<http://www.securityfocus.com/bid/36638>
- \* SECTRACK: 1023007  
<http://securitytracker.com/id?1023007>
- \* VUPEN: ADV-2009-2898  
<http://www.vupen.com/english/advisories/2009/2898>

**CVE Reference:**

CVE-2009-2996 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **14556 Adobe Acrobat / Reader heap overflow Vulnerability (CVE-2009-2997) (Remote File Checking)**

Heap-based buffer overflow in Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 might allow attackers to execute arbitrary code via unspecified vectors.

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

**References:**

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- \* CERT: TA09-286B  
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- \* BID: 36638  
<http://www.securityfocus.com/bid/36638>
- \* SECTRACK: 1023007  
<http://securitytracker.com/id?1023007>
- \* VUPEN: ADV-2009-2898  
<http://www.vupen.com/english/advisories/2009/2898>

**CVE Reference:**

CVE-2009-2997 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 14557 Adobe Acrobat / Reader input validation Vulnerability (CVE-2009-2998) (Remote File Checking)

Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 do not properly validate input, which might allow attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-3458.

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

#### References:

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- \* CERT: TA09-286B  
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- \* BID: 36638  
<http://www.securityfocus.com/bid/36638>
- \* SECTRACK: 1023007  
<http://securitytracker.com/id?1023007>
- \* VUPEN: ADV-2009-2898  
<http://www.vupen.com/english/advisories/2009/2898>

#### CVE Reference:

CVE-2009-2998 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 14558 Adobe Acrobat / Reader stack overflow Vulnerability (CVE-2009-3431) (Remote File Checking)

Stack consumption vulnerability in Adobe Reader and Acrobat 9.1.3, 9.1.2, 9.1.1, and earlier 9.x versions; 8.1.6 and earlier 8.x versions; and possibly 7.1.4 and earlier 7.x versions allows remote attackers to cause a denial of service (application crash) via a PDF file with a large number of [ (open square bracket) characters in the argument to the alert method. NOTE: some of these details are obtained from third party information.

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

#### References:

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- \* CERT: TA09-286B  
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- \* BID: 35148  
<http://www.securityfocus.com/bid/35148>
- \* SECTRACK: 1023007  
<http://securitytracker.com/id?1023007>
- \* VUPEN: ADV-2009-2898  
<http://www.vupen.com/english/advisories/2009/2898>

#### CVE Reference:

CVE-2009-3431 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • 14559 Adobe Acrobat / Reader input validation Vulnerability (CVE-2009-3458) (Remote File Checking)

Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 do not properly validate input, which might allow attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-2998.

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

#### References:

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- \* CERT: TA09-286B  
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- \* BID: 36638  
<http://www.securityfocus.com/bid/36638>
- \* SECTRACK: 1023007  
<http://securitytracker.com/id?1023007>
- \* VUPEN: ADV-2009-2898  
<http://www.vupen.com/english/advisories/2009/2898>

#### CVE Reference:

CVE-2009-3458 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **14560 Adobe Acrobat / Reader heap overflow Vulnerability (CVE-2009-3459) (Remote File Checking)**

Heap-based buffer overflow in Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 allows remote attackers to execute arbitrary code via a crafted PDF file that triggers memory corruption, as exploited in the wild in October 2009. NOTE: some of these details are obtained from third party information.

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

**References:**

- \* ISS: 20091009 Adobe Acrobat and Acrobat Reader Remote Code Execution  
<http://www.iss.net/threats/348.html>
- \* MISC:  
<http://isc.sans.org/diary.html?storyid=7300>
- \* CONFIRM:  
[http://blogs.adobe.com/psirt/2009/10/adobe\\_reader\\_and\\_acrobat\\_issue\\_1.html](http://blogs.adobe.com/psirt/2009/10/adobe_reader_and_acrobat_issue_1.html)
- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- \* CERT: TA09-286B  
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- \* BID: 36600  
<http://www.securityfocus.com/bid/36600>
- \* SECTRACK: 1023007  
<http://securitytracker.com/id?1023007>
- \* SECUNIA: 36983  
<http://secunia.com/advisories/36983>
- \* VUPEN: ADV-2009-2851  
<http://www.vupen.com/english/advisories/2009/2851>
- \* VUPEN: ADV-2009-2898  
<http://www.vupen.com/english/advisories/2009/2898>
- \* XF: adobe-reader-pdf-code-execution(53691)  
<http://xforce.iss.net/xforce/xfdb/53691>

**CVE Reference:**

CVE-2009-3459 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **14561 Adobe Acrobat memory corruption Vulnerability (CVE-2009-3460) (Remote File Checking)**

Adobe Acrobat 9.x before 9.2, 8.x before 8.1.7, and possibly 7.x through 7.1.4 allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.

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

**References:**

- \* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>
- \* CERT: TA09-286B  
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>
- \* BID: 36638  
<http://www.securityfocus.com/bid/36638>
- \* SECTRACK: 1023007  
<http://securitytracker.com/id?1023007>
- \* VUPEN: ADV-2009-2898  
<http://www.vupen.com/english/advisories/2009/2898>

**CVE Reference:**

CVE-2009-3460 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

• **14562 Adobe Acrobat bypass file extension security controls Vulnerability (CVE-2009-3461) (Remote File Checking)**

Unspecified vulnerability in Adobe Acrobat 9.x before 9.2 allows attackers to bypass intended file-extension restrictions via unknown vectors.

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

**References:**

\* CONFIRM:  
<http://www.adobe.com/support/security/bulletins/apsb09-15.html>  
\* CERT: TA09-286B  
<http://www.us-cert.gov/cas/techalerts/TA09-286B.html>  
\* BID: 36638  
<http://www.securityfocus.com/bid/36638>  
\* SECTRACK: 1023007  
<http://securitytracker.com/id?1023007>  
\* VUPEN: ADV-2009-2898  
<http://www.vupen.com/english/advisories/2009/2898>

#### CVE Reference:

CVE-2009-3461 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

### • CVE-2010-0040 Apple CVSS 2.0 Score = 9.3

Integer overflow in ColorSync in Apple Safari before 4.0.5 on Windows allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via an image with a crafted color profile that triggers a heap-based buffer overflow. Per: <http://lists.apple.com/archives/security-announce/2010/Mar/msg00000.html>  
ColorSync CVE-ID: CVE-2010-0040 Available for: Windows 7, Vista, XP Impact: Viewing a maliciously crafted image with an embedded color profile may lead to an unexpected application termination or arbitrary code execution  
Description: An integer overflow, that could result in a heap buffer overflow, exists in the handling of images with an embedded color profile. Opening a maliciously crafted image with an embedded color profile may lead to an unexpected application termination or arbitrary code execution. The issue is addressed by performing additional validation of color profiles. This issue does not affect Mac OS X systems. Credit to Sebastien Renaud of VUPEN Vulnerability Research Team for reporting this issue.

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

#### References:

BID: <http://www.securityfocus.com/bid/38674>

BID: <http://www.securityfocus.com/bid/38671>

CONFIRM: <http://support.apple.com/kb/HT4070>

APPLE: <http://lists.apple.com/archives/security-announce/2010/Mar/msg00000.html>

CVE Reference: [CVE-2010-0040](http://cve.mitre.org/cve/2010/0040)

### • CVE-2010-0043 Apple CVSS 2.0 Score = 9.3

ImageIO in Apple Safari before 4.0.5 on Windows allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted TIFF image. Per: <http://lists.apple.com/archives/security-announce/2010/Mar/msg00000.html> 'ImageIO CVE-ID: CVE-2010-0043 Available for: Windows 7, Vista, XP Impact: Processing a maliciously crafted TIFF image may lead to an unexpected application termination or arbitrary code execution Description: A memory corruption issue exists in the handling of TIFF images. Processing a maliciously crafted TIFF image may lead to an unexpected application termination or arbitrary code execution. This issue is addressed through improved memory handling. Credit to Gus Mueller of Flying Meat for reporting this issue.'

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

#### References:

BID: <http://www.securityfocus.com/bid/38673>

BID: <http://www.securityfocus.com/bid/38671>

CONFIRM: <http://support.apple.com/kb/HT4070>

APPLE: <http://lists.apple.com/archives/security-announce/2010/Mar/msg00000.html>

CVE Reference: [CVE-2010-0043](http://cve.mitre.org/cve/2010/0043)

### • CVE-2010-0045 Apple CVSS 2.0 Score = 9.3

Apple Safari before 4.0.5 on Windows does not properly validate external URL schemes, which allows remote attackers to open local files and execute arbitrary code via a crafted HTML document. Per: <http://lists.apple.com/archives/security-announce/2010/Mar/msg00000.html> CVE-ID: CVE-2010-0045 Available for: Windows 7, Vista, XP Impact: Visiting a maliciously crafted website may lead to arbitrary code execution Description: An issue in Safari's handling of external URL schemes may cause a local file to be opened in response to a URL encountered on a web page. Visiting a maliciously crafted website may lead to arbitrary code execution. This update addresses the issue through improved validation of external URLs. This issue does not affect Mac OS X systems. Credit to Billy Rios and Microsoft Vulnerability Research (MSVR) for reporting this issue.

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

**References:**

BID: <http://www.securityfocus.com/bid/38671>

CONFIRM: <http://support.apple.com/kb/HT4070>

APPLE: <http://lists.apple.com/archives/security-announce/2010/Mar/msg00000.html>

**CVE Reference:** [CVE-2010-0045](#)

• **CVE-2010-0046 Apple CVSS 2.0 Score = 9.3**

The Cascading Style Sheets (CSS) implementation in WebKit in Apple Safari before 4.0.5 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via crafted format arguments. Per: <http://lists.apple.com/archives/security-announce/2010/Mar/msg00000.html> 'WebKit CVE-ID: CVE-2010-0046 Available for: Mac OS X v10.4.11, Mac OS X Server v10.4.11, Mac OS X v10.5.8, Mac OS X Server v10.5.8, Mac OS X v10.6.1 or later, Mac OS X Server v10.6.1 or later, Windows 7, Vista, XP Impact: Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution Description: A memory corruption issue exists in WebKit's handling of CSS format() arguments. Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution. This issue is addressed through improved handling of CSS format() arguments. Credit to Robert Swiecki of Google Inc. for reporting this issue.'

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

**References:**

BID: <http://www.securityfocus.com/bid/38671>

CONFIRM: <http://support.apple.com/kb/HT4070>

APPLE: <http://lists.apple.com/archives/security-announce/2010/Mar/msg00000.html>

**CVE Reference:** [CVE-2010-0046](#)

• **CVE-2010-0047 Apple CVSS 2.0 Score = 9.3**

Use-after-free vulnerability in WebKit in Apple Safari before 4.0.5 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors related to "HTML object element fallback content." Per: <http://lists.apple.com/archives/security-announce/2010/Mar/msg00000.html> 'WebKit CVE-ID: CVE-2010-0047 Available for: Mac OS X v10.4.11, Mac OS X Server v10.4.11, Mac OS X v10.5.8, Mac OS X Server v10.5.8, Mac OS X v10.6.1 or later, Mac OS X Server v10.6.1 or later, Windows 7, Vista, XP Impact: Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution Description: A use-after-free issue exists in the handling of HTML object element fallback content. Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution. This issue is addressed through improved memory reference tracking. Credit to wushi of team509, working with TippingPoint's Zero Day Initiative for reporting this issue.'

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

**References:**

BID: <http://www.securityfocus.com/bid/38671>

CONFIRM: <http://support.apple.com/kb/HT4070>

APPLE: <http://lists.apple.com/archives/security-announce/2010/Mar/msg00000.html>

**CVE Reference:** [CVE-2010-0047](#)

• **CVE-2010-0048 Apple CVSS 2.0 Score = 9.3**

Use-after-free vulnerability in WebKit in Apple Safari before 4.0.5 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted XML document. Per:

<http://lists.apple.com/archives/security-announce/2010/Mar/msg00000.html> CVE-ID: CVE-2010-0048 Available for: Mac OS X v10.4.11, Mac OS X Server v10.4.11, Mac OS X v10.5.8, Mac OS X Server v10.5.8, Mac OS X v10.6.1 or later, Mac OS X Server v10.6.1 or later, Windows 7, Vista, XP Impact: Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution Description: A use-after-free issue exists in WebKit's parsing of XML documents. Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution. This issue is addressed through improved memory reference tracking.

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

**References:**

BID: <http://www.securityfocus.com/bid/38671>

CONFIRM: <http://support.apple.com/kb/HT4070>

APPLE: <http://lists.apple.com/archives/security-announce/2010/Mar/msg00000.html>

**CVE Reference:** [CVE-2010-0048](#)

• **CVE-2010-0049 Apple CVSS 2.0 Score = 9.3**

Use-after-free vulnerability in WebKit in Apple Safari before 4.0.5 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via HTML elements with right-to-left (RTL) text directionality. Per: <http://lists.apple.com/archives/security-announce/2010/Mar/msg00000.html> CVE-ID: CVE-2010-0049 Available for: Mac OS X v10.4.11, Mac OS X Server v10.4.11, Mac OS X v10.5.8, Mac OS X Server v10.5.8, Mac OS X v10.6.1 or later, Mac OS X Server v10.6.1 or later, Windows 7, Vista, XP Impact: Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution Description: A use-after-free issue exists in the handling of HTML elements containing right-to-left displayed text. Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution. This issue is addressed through improved memory reference tracking. Credit to wushi&Z of team509 for reporting this issue.

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

**References:**

BID: <http://www.securityfocus.com/bid/38671>

CONFIRM: <http://support.apple.com/kb/HT4070>

APPLE: <http://lists.apple.com/archives/security-announce/2010/Mar/msg00000.html>

**CVE Reference:** [CVE-2010-0049](#)

• **CVE-2010-0050 Apple CVSS 2.0 Score = 9.3**

Use-after-free vulnerability in WebKit in Apple Safari before 4.0.5 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via an HTML document with improperly nested tags. Per: <http://lists.apple.com/archives/security-announce/2010/Mar/msg00000.html> 'WebKit CVE-ID: CVE-2010-0050 Available for: Mac OS X v10.4.11, Mac OS X Server v10.4.11, Mac OS X v10.5.8, Mac OS X Server v10.5.8, Mac OS X v10.6.1 or later, Mac OS X Server v10.6.1 or later, Windows 7, Vista, XP Impact: Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution Description: A use-after-free issue exists in WebKit's handling of incorrectly nested HTML tags. Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution. This issue is addressed through improved memory reference tracking. Credit to wushi&Z of team509 working with TippingPoint's Zero Day Initiative for reporting this issue.'

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

**References:**

BID: <http://www.securityfocus.com/bid/38671>

CONFIRM: <http://support.apple.com/kb/HT4070>

APPLE: <http://lists.apple.com/archives/security-announce/2010/Mar/msg00000.html>

**CVE Reference:** [CVE-2010-0050](#)

**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)