

## 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

Fast growing new botnet. Google hackers may be active again. Risky searching. 3rd party fix for Adobe 0-day.

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

### • New commercial DDoS botnet discovered

Researchers have discovered a fast-growing botnet that was designed as part of a commercial service for launching distributed denial-of-service (DDoS) attacks against any target. The "IMDDOS" botnet, named after the website promoting its DDoS attack services, dates back to March 20 when a criminal organization registered a series of domains to serve as the botnet's command-and-control (C&C) hubs, according to a report issued Monday by security firm Damballa.

Growing at a rate of as many as 10,000 new victims each day, IMDDOS became one of the largest active botnets in the world in fewer than four months, David Holmes, vice president of marketing at Damballa, told SCMagazineUS.com on Tuesday.

The botnet can be leased to launch DDoS attacks, which use a large number of compromised PCs, or bots, to flood a targeted website with requests, causing it to become unresponsive. SC Magazine

Full Story :

[http://www.scmagazineus.com/new-commercial-ddos-botnet-discovered/article/178882/?utm\\_source=feedburner&utm\\_medium=feedburner](http://www.scmagazineus.com/new-commercial-ddos-botnet-discovered/article/178882/?utm_source=feedburner&utm_medium=feedburner)

## • Researchers clash over possible return of Google attackers

Computerworld - Researchers on Monday clashed over whether recent attacks that exploit a bug in Adobe Reader are the work of the group that hacked Google and dozens of other major corporations late last year.

On one side, Mountain View, Calif.-based antivirus giant Symantec, whose security analysts said they've found evidence suggesting that the group which wormed its way into Google's corporate network in December 2009 is back in business.

On the other, Atlanta's much smaller SecureWorks, where researcher Don Jackson said that Symantec had "comingled" evidence of two separate attacks. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9185281/Researchers\\_clash\\_over\\_possible\\_return\\_of\\_Google\\_attackers?sc](http://www.computerworld.com/s/article/9185281/Researchers_clash_over_possible_return_of_Google_attackers?sc)

## • Searching for free stuff online can be costly

This pie chart shows the different threats that can come from visiting Web sites that advertise unauthorized content.

(Credit: McAfee)

It's common knowledge that you can catch computer viruses on porn Web sites. But did you know it's also risky to surf the Web searching for free movies or music? Cnet Security

Full Story :

[http://news.cnet.com/8301-27080\\_3-20016309-245.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-27080_3-20016309-245.html?part=rss&subj=news&tag=2547-1_3-0-20)

## • Researchers issue homemade patch for PDF zero-day bug

Computerworld - A little-known security firm on Wednesday released a home-brewed patch for a critical bug in Adobe Reader that hackers are already exploiting.

RamzAfzar, whose Web site bills it as a penetration testing company, reworked a flawed Adobe dynamic link library, or DLL, to replace the vulnerable "strcat" API call with the more secure alternative, "strncat."

This isn't the first time that someone has beat Adobe to a patch for Reader. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9186420/Researchers\\_issue\\_homemade\\_patch\\_for\\_PDF\\_zero\\_day\\_bug?sc](http://www.computerworld.com/s/article/9186420/Researchers_issue_homemade_patch_for_PDF_zero_day_bug?sc)

# New Vulnerabilities Tested in SecureScout

## • 18926 QuickTime heap buffer overflow exists in the handling of FLC encoded movie files (Remote File Checking)

A heap buffer overflow exists in the handling of FLC encoded movie files. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This issue is addressed by performing additional validation of FLC encoded movie files.

The issue has been fixed in version 7.6.6.

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

### References:

\* BUGTRAQ: 20100402 ZDI-10-044: Apple QuickTime FLI LinePacket Remote Code Execution Vulnerability  
<http://www.securityfocus.com/archive/1/archive/1/510520/100/0/threaded>

\* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-10-044>

\* CONFIRM:

<http://support.apple.com/kb/HT4077>

\* APPLE: APPLE-SA-2010-03-29-1

<http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>

\* APPLE: APPLE-SA-2010-03-30-1

<http://lists.apple.com/archives/security-announce/2010/Mar/msg00002.html>

\* OVAL: oval:org.mitre.oval:def:6801

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6801>

### CVE Reference:

CVE-2010-0520 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • **18927 QuickTime heap buffer overflow exists in the handling of MPEG encoded movie files (Remote File Checking)**

A heap buffer overflow exists in the handling of MPEG encoded movie files. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This issue is addressed by performing additional validation of MPEG encoded movie files.

The issue has been fixed in version 7.6.6.

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

#### References:

- \* BUGTRAQ: 20100402 ZDI-10-035: Apple QuickTime genl Atom Remote Code Execution Vulnerability  
<http://www.securityfocus.com/archive/1/archive/1/510508/100/0/threaded>
- \* BUGTRAQ: 20100402 ZDI-10-045: Apple QuickTime MPEG-1 genl Atom Remote Code Execution Vulnerability  
<http://www.securityfocus.com/archive/1/archive/1/510530/100/0/threaded>
- \* MISC:  
<http://www.zerodayinitiative.com/advisories/ZDI-10-035>
- \* MISC:  
<http://www.zerodayinitiative.com/advisories/ZDI-10-045>
- \* CONFIRM:  
<http://support.apple.com/kb/HT4077>
- \* APPLE: APPLE-SA-2010-03-29-1  
<http://lists.apple.com/archives/security-announce/2010/Mar/msg00001.html>
- \* APPLE: APPLE-SA-2010-03-30-1  
<http://lists.apple.com/archives/security-announce/2010/Mar/msg00002.html>
- \* OVAL: oval:org.mitre.oval:def:6927  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6927>

#### CVE Reference:

CVE-2010-0526 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • **18928 QuickTime integer overflow exists in the handling of PICT images (Remote File Checking)**

An integer overflow exists in the handling of PICT images. Opening a maliciously crafted PICT image may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue by performing additional validation of PICT images.

The issue has been fixed in version 7.6.6.

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

#### References:

- \* APPLE: APPLE-SA-2010-03-30-1  
<http://lists.apple.com/archives/security-announce/2010/Mar/msg00002.html>
- \* OVAL: oval:org.mitre.oval:def:7458  
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7458>

#### CVE Reference:

CVE-2010-0527 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

### • **18929 QuickTime memory corruption exists in the handling of color tables in movie files (Remote File Checking)**

A memory corruption exists in the handling of color tables in movie files. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution. This issue is addressed by performing additional validation of color tables.

The issue has been fixed in version 7.6.6.

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

#### References:

- \* BUGTRAQ: 20100402 ZDI-10-042: Apple QuickTime MediaVideo Compressor Name Remote Code Execution Vulnerability  
<http://www.securityfocus.com/archive/1/archive/1/510518/100/0/threaded>
- \* MISC:  
<http://www.zerodayinitiative.com/advisories/ZDI-10-042>
- \* APPLE: APPLE-SA-2010-03-30-1

<http://lists.apple.com/archives/security-announce/2010//Mar/msg00002.html>

\* OVAL: oval:org.mitre.oval:def:6989

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6989>

#### CVE Reference:

CVE-2010-0528 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18930 QuickTime heap buffer overflow exists in the handling of PICT images (CVE-2010-0529) (Remote File Checking)

A heap buffer overflow exists in the handling of PICT images. Opening a maliciously crafted PICT image may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue by performing additional validation of PICT images.

The issue has been fixed in version 7.6.6.

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

#### References:

\* BUGTRAQ: 20100406 ZDI-10-067: Apple QuickTime Pict BkPixPat Remote Code Execution Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/510569/100/0/threaded>

\* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-10-067>

\* APPLE: APPLE-SA-2010-03-30-1

<http://lists.apple.com/archives/security-announce/2010//Mar/msg00002.html>

\* OVAL: oval:org.mitre.oval:def:6780

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6780>

#### CVE Reference:

CVE-2010-0529 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18931 QuickTime memory corruption issue exists in the handling of BMP images (Remote File Checking)

A memory corruption issue exists in the handling of BMP images. Opening a maliciously crafted BMP image may lead to an unexpected application termination or arbitrary code execution. This update addresses the issue by performing additional validation of BMP images.

The issue has been fixed in version 7.6.6.

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

#### References:

\* BUGTRAQ: 20100406 ZDI-10-067: Apple QuickTime Pict BkPixPat Remote Code Execution Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/510569/100/0/threaded>

\* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-10-067>

\* APPLE: APPLE-SA-2010-03-30-1

<http://lists.apple.com/archives/security-announce/2010//Mar/msg00002.html>

\* OVAL: oval:org.mitre.oval:def:6780

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:6780>

#### CVE Reference:

CVE-2010-0529 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

#### • 18932 Print Spooler Service Impersonation Vulnerability (MS10-061/2347290) (Remote File Checking)

A remote code execution vulnerability exists in the Windows Print Spooler service that could allow a remote, unauthenticated attacker to execute arbitrary code on an affected Windows XP system. 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. This is an elevation of privilege vulnerability on all other supported Microsoft Windows systems.

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

#### References:

\* MS: MS10-061

<http://www.microsoft.com/technet/security/bulletin/ms10-061.msp>

\* VUPEN: VUPEN/ADV-2010-2382  
<http://www.vupen.com/english/advisories/2010/2382>  
\* SECTRACK: 1024435  
<http://securitytracker.com/alerts/2010/Sep/1024435.html>  
\* BID: 43073  
<http://www.securityfocus.com/bid/43073>

**CVE Reference:**

CVE-2010-2729 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **18933 MPEG-4 Codec Vulnerability (MS10-062/975558) (Remote File Checking)**

A remote code execution vulnerability exists in the way that the MPEG-4 codec handles supported format files. This vulnerability could allow code execution if a user opened a specially crafted media file. 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

**References:**

\* MS: MS10-062  
<http://www.microsoft.com/technet/security/bulletin/ms10-062.msp>  
\* VUPEN: VUPEN/ADV-2010-2383  
<http://www.vupen.com/english/advisories/2010/2383>  
\* SECTRACK: 1024436  
<http://securitytracker.com/alerts/2010/Sep/1024436.html>

**CVE Reference:**

CVE-2010-0818 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **18934 Uniscribe Font Parsing Engine Memory Corruption Vulnerability (MS10-063/2320113) (Remote File Checking)**

A remote code execution vulnerability exists in affected versions of Microsoft Windows and Microsoft Office. The vulnerability exists because Windows and Office incorrectly parse specific font types in such a way that could allow remote code execution. An attacker who successfully exploited this vulnerability could run arbitrary code as the logged-on user.

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

**References:**

\* MS: MS10-063  
<http://www.microsoft.com/technet/security/bulletin/ms10-063.msp>  
\* VUPEN: VUPEN/ADV-2010-2384  
<http://www.vupen.com/english/advisories/2010/2384>  
\* SECTRACK: 1024437  
<http://securitytracker.com/alerts/2010/Sep/1024437.html>  
\* BID: 43068  
<http://www.securityfocus.com/bid/43068>

**CVE Reference:**

CVE-2010-2738 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

● **18935 Heap Based Buffer Overflow in Outlook Vulnerability (MS10-064/2315011) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Outlook parses content in a specially crafted e-mail message. This vulnerability exists only in configurations where Outlook connects to an Exchange Server in Online Mode. Configurations where Outlook connects to an Exchange Server in the Cached Exchange Mode are not affected. In addition, configurations where Outlook uses POP or IMAP mail servers only are not affected by this vulnerability. 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: MS10-064

<http://www.microsoft.com/technet/security/bulletin/ms10-064.mspx>

\* VUPEN: VUPEN/ADV-2010-2385

<http://www.vupen.com/english/advisories/2010/2385>

\* SECTRACK: 1024439

<http://securitytracker.com/alerts/2010/Sep/1024439.html>

\* BID: 43063

<http://www.securityfocus.com/bid/43063>

#### CVE Reference:

CVE-2010-2728 ([cve.mitre.org](http://cve.mitre.org), [nvd.nist.gov](http://nvd.nist.gov))

## New Vulnerabilities found this Week

### • CVE-2010-0818 Microsoft CVSS 2.0 Score = 9.3

The MPEG-4 codec in the Windows Media codecs in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 Gold and SP2 does not properly handle crafted media content with MPEG-4 video encoding, which allows remote attackers to execute arbitrary code via a file in an unspecified "supported format," aka "MPEG-4 Codec Vulnerability."

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

#### References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-062.mspx>

CVE Reference: [CVE-2010-0818](http://cve.mitre.org/cve/2010/0818)

### • CVE-2010-2563 Microsoft CVSS 2.0 Score = 9.3

The Word 97 text converter in the WordPad Text Converters in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly parse malformed structures in Word 97 documents, which allows remote attackers to execute arbitrary code via a crafted document, aka "WordPad Word 97 Text Converter Memory Corruption Vulnerability."

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

#### References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-067.mspx>

CVE Reference: [CVE-2010-2563](http://cve.mitre.org/cve/2010/2563)

### • CVE-2010-2567 Microsoft CVSS 2.0 Score = 9.3

The RPC client implementation in Microsoft Windows XP SP2 and SP3 and Server 2003 SP2 does not properly allocate memory during the parsing of responses, which allows remote RPC servers and man-in-the-middle attackers to execute arbitrary code via a malformed response, aka "RPC Memory Corruption Vulnerability."

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

#### References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-066.mspx>

CVE Reference: [CVE-2010-2567](http://cve.mitre.org/cve/2010/2567)

### • CVE-2010-2728 Microsoft CVSS 2.0 Score = 9.3

Heap-based buffer overflow in Microsoft Outlook 2002 SP3, 2003 SP3, and 2007 SP2, when Online Mode for an Exchange Server is enabled, allows remote attackers to execute arbitrary code via a crafted e-mail message, aka "Heap Based Buffer Overflow in Outlook Vulnerability."

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

#### References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-064.mspx>

CVE Reference: [CVE-2010-2728](http://cve.mitre.org/cve/2010/2728)

### • CVE-2010-2729 Microsoft CVSS 2.0 Score = 9.3

The Print Spooler service 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, when printer sharing is enabled, does not properly validate spooler access permissions, which allows remote attackers to create files in a system directory, and consequently execute arbitrary code, by sending a crafted print request over RPC, as exploited in the wild in September 2010, aka "Print Spooler Service Impersonation Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-061.msp>

**CVE Reference:** [CVE-2010-2729](#)

• **CVE-2010-2730 Microsoft CVSS 2.0 Score = 9.3**

Buffer overflow in Microsoft Internet Information Services (IIS) 7.5, when FastCGI is enabled, allows remote attackers to execute arbitrary code via crafted headers in a request, aka "Request Header Buffer Overflow Vulnerability." Per: <http://www.microsoft.com/technet/security/Bulletin/MS10-065.msp> 'FastCGI is not enabled by default in IIS.'

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-065.msp>

**CVE Reference:** [CVE-2010-2730](#)

• **CVE-2010-2738 Microsoft CVSS 2.0 Score = 9.3**

The Uniscribe (aka new Unicode Script Processor) implementation in USP10.DLL in Microsoft Windows XP SP2 and SP3, Server 2003 SP2, Vista SP1 and SP2, and Server 2008 Gold and SP2, and Microsoft Office XP SP3, 2003 SP3, and 2007 SP2, does not properly validate tables associated with malformed OpenType fonts, which allows remote attackers to execute arbitrary code via a crafted (1) web site or (2) Office document, aka "Uniscribe Font Parsing Engine Memory Corruption Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-063.msp>

**CVE Reference:** [CVE-2010-2738](#)

• **CVE-2010-0820 Microsoft CVSS 2.0 Score = 9.0**

Heap-based buffer overflow in the Local Security Authority Subsystem Service (LSASS), as used in Active Directory in Microsoft Windows Server 2003 SP2 and Windows Server 2008 Gold, SP2, and R2; Active Directory Application Mode (ADAM) in Windows XP SP2 and SP3 and Windows Server 2003 SP2; and Active Directory Lightweight Directory Service (AD LDS) in Windows Vista SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7, allows remote authenticated users to execute arbitrary code via malformed LDAP messages, aka "LSASS Heap Overflow Vulnerability."

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

**References:**

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-068.msp>

**CVE Reference:** [CVE-2010-0820](#)

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