

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

Huge 'drive by' attack. Acquisitions a problem for innovation. AV solutions fail to find known vulnerabilities in test. 'There's no such thing as perfect protection.'

Enjoy reading & Stay safe.

Call or email netVigilance to get an update on SecureScout.

(503) 524 5758 or sales@netvigilance.com

Top Security News Stories this Week

• Malicious widget hacked millions of Web sites

Computerworld - As many as five million Web sites hosted by Network Solutions have been serving up malware, probably for several months, a security expert said today.

"This is one of the biggest infections for drive-by download attacks that I've seen," said Wayne Huang, co-founder and CTO of Santa Clara, Calif.-based Armorize Technologies, a Web application security company.

Network Solutions disputed Huang's estimate of between 500,000 and 5 million infected sites, but was unable to provide its own count. Computerworld

Full Story :

http://www.computerworld.com/s/article/9180783/Malicious_widget_hacked_millions_of_Web_sites?source=rss_sec

• Acquisitions blunt security innovation, say users, analysts

Computerworld - Some IT managers and analysts said the planned \$7.7 billion Intel-McAfee deal and Hewlett-Packard's acquisition of Fortify this week are the latest examples of a trend that could threaten long-term innovation in the security industry.

This week's moves are the latest in a long line of merger and acquisition activity in the security industry in recent years.

The McAfee acquisition marks a completely unexpected entry into the security market by Intel. But the chip giant's move follows similar ones by other major vendors like IBM, Cisco, EMC and Symantec -- and HP -- to pick up security vendors. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9181040/Acquisitions blunt security innovation say users analysts?source=rss_security](http://www.computerworld.com/s/article/9181040/Acquisitions_blunt_security_innovation_say_users_analysts?source=rss_security)

• **NSS Labs: Testing shows most AV suites fail against exploits**

IDG News Service - A majority of security software suites still fail to detect attacks on PCs even after the style of attack has been known for some time, underscoring how cybercriminals still have the upper hand.

NSS Labs, which conducts tests of security software suites, tested how security packages from 10 major companies detect so-called "client-side exploits." In such incidents a hacker attacks a vulnerability in software such as Web browsers, browser plug-ins or desktop applications such as Adobe Acrobat and Flash.

NSS Labs is an independent security software company that unlike many other testing companies does not accept vendor money for performing comparative evaluations. Vendors are notified, however, and are allowed to make some configuration changes before NSS Labs' evaluation. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9180823/NSS Labs Testing shows most AV suites fail against exploits?source=rss_security](http://www.computerworld.com/s/article/9180823/NSS_Labs_Testing_shows_most_AV_suites_fail_against_exploits?source=rss_security)

• **How Did My Protected PC Get Infected?**

PC World - SUPERAntiSpyware found three Trojans on Bill Artman's PC. Bill asked the Windows forum how this could happen when his PC is protected.

There's no such thing as perfect protection. Even if you have the best firewall and antivirus software available, and keep it up to date, something might get through. But knowing how they'll get through can help you block them.

First, do you really have the best security software? Windows' own firewall, for instance, doesn't protect as well as a good, third-party firewall. I currently use Comodo's free firewall (there's a separate x64 version). It's an annoying product, constantly interrupting my work to ask if I should allow something or other to get through, but the security is worth it. Computerworld

Full Story :

[http://www.computerworld.com/s/article/9180772/How Did My Protected PC Get Infected ?source=rss_security](http://www.computerworld.com/s/article/9180772/How_Did_My_Protected_PC_Get_Infected_?source=rss_security)

New Vulnerabilities Tested in SecureScout

• **18883 Word Record Parsing Vulnerability (MS10-056/2269638) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office Word handles malformed records inside a specially crafted Word file. 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: MS10-056

<http://www.microsoft.com/technet/security/Bulletin/MS10-056.mspx>

* BID: 42136

<http://www.securityfocus.com/bid/42136>

* VUPEN: VUPEN/ADV-2010-2053

<http://www.vupen.com/english/advisories/2010/2053>

* SECTRAK: 1024298

<http://securitytracker.com/alerts/2010/Aug/1024298.html>

CVE Reference:

CVE-2010-1900 (cve.mitre.org, nvd.nist.gov)

• **18884 Word RTF Parsing Engine Memory Corruption Vulnerability (MS10-056/2269638) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office Word parses rich text data. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. 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: MS10-056
<http://www.microsoft.com/technet/security/Bulletin/MS10-056.msp>
- * BID: 42132
<http://www.securityfocus.com/bid/42132>
- * VUPEN: VUPEN/ADV-2010-2053
<http://www.vupen.com/english/advisories/2010/2053>
- * SECTRACK: 1024298
<http://securitytracker.com/alerts/2010/Aug/1024298.html>

CVE Reference:

CVE-2010-1901 (cve.mitre.org, nvd.nist.gov)

• **18885 Word RTF Parsing Buffer Overflow Vulnerability (MS10-056/2269638) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office Word parses certain rich text data. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. 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: MS10-056
<http://www.microsoft.com/technet/security/Bulletin/MS10-056.msp>
- * BID: 42133
<http://www.securityfocus.com/bid/42133>
- * VUPEN: VUPEN/ADV-2010-2053
<http://www.vupen.com/english/advisories/2010/2053>
- * SECTRACK: 1024298
<http://securitytracker.com/alerts/2010/Aug/1024298.html>

CVE Reference:

CVE-2010-1902 (cve.mitre.org, nvd.nist.gov)

• **18886 Word HTML Linked Objects Memory Corruption Vulnerability (MS10-056/2269638) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office Word handles a specially crafted Word file that includes a malformed record. 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: MS10-056
<http://www.microsoft.com/technet/security/Bulletin/MS10-056.msp>
- * BID: 42130
<http://www.securityfocus.com/bid/42130>
- * VUPEN: VUPEN/ADV-2010-2053
<http://www.vupen.com/english/advisories/2010/2053>
- * SECTRACK: 1024298
<http://securitytracker.com/alerts/2010/Aug/1024298.html>

CVE Reference:

CVE-2010-1903 (cve.mitre.org, nvd.nist.gov)

• **18887 Windows Kernel Data Initialization Vulnerability (MS10-047/981852) (Remote File Checking)**

An elevation of privilege vulnerability exists in the Windows Kernel due to the way the kernel deals with specific thread creation attempts. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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: **Medium**

References:

- * MS: MS10-047
<http://www.microsoft.com/technet/security/Bulletin/MS10-047.msp>
- * BID: 42211
<http://www.securityfocus.com/bid/42211>
- * VUPEN: VUPEN/ADV-2010-2044
<http://www.vupen.com/english/advisories/2010/2044>
- * SECTRACK: 1024307
<http://securitytracker.com/alerts/2010/Aug/1024307.html>

CVE Reference:

CVE-2010-1888 (cve.mitre.org, nvd.nist.gov)

• **18888 Windows Kernel Double Free Vulnerability (MS10-047/981852) (Remote File Checking)**

An elevation of privilege vulnerability exists in the Windows Kernel due to the way the kernel initializes objects while handling certain errors. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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: **Medium**

References:

- * MS: MS10-047
<http://www.microsoft.com/technet/security/Bulletin/MS10-047.msp>
- * BID: 42213
<http://www.securityfocus.com/bid/42213>
- * VUPEN: VUPEN/ADV-2010-2044
<http://www.vupen.com/english/advisories/2010/2044>
- * SECTRACK: 1024307
<http://securitytracker.com/alerts/2010/Aug/1024307.html>

CVE Reference:

CVE-2010-1889 (cve.mitre.org, nvd.nist.gov)

• **18889 Windows Kernel Improper Validation Vulnerability (MS10-047/981852) (Remote File Checking)**

A denial of service vulnerability exists in the way that the Windows kernel validates access control lists on kernel objects. An attacker could exploit the vulnerability by running a specially crafted application causing the system to become unresponsive and automatically restart.

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

References:

- * MS: MS10-047
<http://www.microsoft.com/technet/security/Bulletin/MS10-047.msp>
- * BID: 42221
<http://www.securityfocus.com/bid/42221>
- * VUPEN: VUPEN/ADV-2010-2044
<http://www.vupen.com/english/advisories/2010/2044>
- * SECTRACK: 1024307
<http://securitytracker.com/alerts/2010/Aug/1024307.html>

CVE Reference:

CVE-2010-1890 (cve.mitre.org, nvd.nist.gov)

• **18890 Win32k Bounds Checking Vulnerability (MS10-048/2160329) (Remote File Checking)**

A denial of service vulnerability exists in the Windows kernel-mode drivers due to the improper validation of an argument passed to a system call. An attacker could exploit the vulnerability by running a specially crafted application causing the system to become unresponsive and automatically restart.

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

References:

- * MS: MS10-048
<http://www.microsoft.com/technet/security/Bulletin/MS10-048.msp>
- * BID: 42250
<http://www.securityfocus.com/bid/42250>
- * VUPEN: VUPEN/ADV-2010-2045
<http://www.vupen.com/english/advisories/2010/2045>
- * SECTRACK: 1024308
<http://securitytracker.com/alerts/2010/Aug/1024308.html>

CVE Reference:

CVE-2010-1887 (cve.mitre.org, nvd.nist.gov)

• 18891 Win32k Exception Handling Vulnerability (MS10-048/2160329) (Remote File Checking)

An elevation of privilege vulnerability exists due to the way the Windows kernel-mode drivers handle certain exceptions. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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 / Gain Root** Risk: **Medium**

References:

- * MS: MS10-048
<http://www.microsoft.com/technet/security/Bulletin/MS10-048.msp>
- * BID: 39630
<http://www.securityfocus.com/bid/39630>
- * VUPEN: VUPEN/ADV-2010-2045
<http://www.vupen.com/english/advisories/2010/2045>
- * SECTRACK: 1024308
<http://securitytracker.com/alerts/2010/Aug/1024308.html>

CVE Reference:

CVE-2010-1894 (cve.mitre.org, nvd.nist.gov)

• 18892 Win32k Pool Overflow Vulnerability (MS10-048/2160329) (Remote File Checking)

An elevation of privilege vulnerability exists because the Windows kernel-mode drivers do not properly allocate memory when making a copy from user mode. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. 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 / Gain Root** Risk: **Medium**

References:

- * MS: MS10-048
<http://www.microsoft.com/technet/security/Bulletin/MS10-048.msp>
- * BID: 42245
<http://www.securityfocus.com/bid/42245>
- * VUPEN: VUPEN/ADV-2010-2045
<http://www.vupen.com/english/advisories/2010/2045>
- * SECTRACK: 1024308
<http://securitytracker.com/alerts/2010/Aug/1024308.html>

CVE Reference:

CVE-2010-1895 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2010-1886** Microsoft CVSS 2.0 Score = 6.8

Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 SP2 and R2, and Windows 7 allow local users to gain privileges by leveraging access to a process with NetworkService credentials, as demonstrated by TAPI Server, SQL Server, and IIS processes, and related to the Windows Service Isolation feature. NOTE: the vendor states that privilege escalation from NetworkService to LocalSystem does not cross a "security boundary."

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

MSKB: <http://support.microsoft.com/kb/982316>

MSKB: <http://support.microsoft.com/kb/2264072>

CONFIRM: <http://www.microsoft.com/technet/security/advisory/2264072.msp>

CVE Reference: [CVE-2010-1886](#)

• **CVE-2010-1870 Apache CVSS 2.0 Score = 5.0**

The OGNL extensive expression evaluation capability in XWork in Struts 2.0.0 through 2.1.8.1, as used in Atlassian Fisheye, Crucible, and possibly other products, uses a permissive whitelist, which allows remote attackers to modify server-side context objects and bypass the "#" protection mechanism in ParameterInterceptors via the (1) #context, (2) #_memberAccess, (3) #root, (4) #this, (5) #_typeResolver, (6) #_classResolver, (7) #_traceEvaluations, (8) #_lastEvaluation, (9) #_keepLastEvaluation, and possibly other OGNL context variables, a different vulnerability than CVE-2008-6504.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

BID: <http://www.securityfocus.com/bid/41592>

OSVDB: <http://www.osvdb.org/66280>

EXPLOIT-DB: <http://www.exploit-db.com/exploits/14360>

CONFIRM: <http://struts.apache.org/2.2.1/docs/s2-005.html>

FULLDISC: <http://seclists.org/fulldisclosure/2010/Jul/183>

CONFIRM: <http://confluence.atlassian.com/display/FISHEYE/FishEye+Security+Advisory+2010-06-16>

MISC: <http://blog.o0o.nu/2010/07/cve-2010-1870-struts2xwork-remote.html>

CVE Reference: [CVE-2010-1870](#)

• **CVE-2009-3737 Oracle CVSS 2.0 Score = 9.3**

The Oracle Siebel Option Pack for IE ActiveX control does not properly initialize memory that is used by the NewBusObj method, which allows remote attackers to execute arbitrary code via a crafted HTML document.

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

References:

CERT-VN: <http://www.kb.cert.org/vuls/id/174089>

VUPEN: <http://www.vupen.com/english/advisories/2010/2028>

OSVDB: <http://www.osvdb.org/66926>

SECUNIA: <http://secunia.com/advisories/40804>

CVE Reference: [CVE-2009-3737](#)

• **CVE-2010-2826 Cisco CVSS 2.0 Score = 9.0**

SQL injection vulnerability in Cisco Wireless Control System (WCS) 6.0.x before 6.0.196.0 allows remote authenticated users to execute arbitrary SQL commands via vectors related to the ORDER BY clause of the Client List screens, aka Bug ID CSCtf37019.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4091e.shtml

CVE Reference: [CVE-2010-2826](#)

• **CVE-2010-2827 Cisco CVSS 2.0 Score = 7.8**

Cisco IOS 15.1(2)T allows remote attackers to cause a denial of service (resource consumption and TCP outage) via spoofed TCP packets, related to embryonic TCP connections that remain in the SYN_RCVD or SYN_SENT state, aka Bug ID CSCti18193.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4095e.shtml

CVE Reference: [CVE-2010-2827](#)

• **CVE-2010-2822 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability in the RTSP inspection feature on the Cisco Application Control Engine (ACE) Module with software before A2(3.2) for Catalyst 6500 series switches and 7600 series routers, and the Cisco Application Control Engine (ACE) 4710 appliance with software before A3(2.6), allows remote attackers to cause a denial of service (device reload) via crafted RTSP packets over TCP, aka Bug IDs CSCta85227 and CSCtg14858.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4091d.shtml

CVE Reference: [CVE-2010-2822](#)

• **CVE-2010-2823 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability in the deep packet inspection feature on the Cisco Application Control Engine (ACE) 4710 appliance with software before A3(2.6) allows remote attackers to cause a denial of service (device reload) via crafted HTTP packets, related to HTTP, RTSP, and SIP inspection, aka Bug ID CSCtb54493.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4091d.shtml

CVE Reference: [CVE-2010-2823](#)

• **CVE-2010-2824 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability on the Cisco Application Control Engine (ACE) Module with software A2(1.x) before A2(1.6), A2(2.x) before A2(2.3), and A2(3.x) before A2(3.1) for Catalyst 6500 series switches and 7600 series routers allows remote attackers to cause a denial of service (device reload) via a sequence of SSL packets, aka Bug ID CSCta20756.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4091d.shtml

CVE Reference: [CVE-2010-2824](#)

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

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

Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at info-scanner@seurescout.net