

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

\$6 billion cost for health care breaches. Vulnerabilities are inside the network, also. Add-on addresses the perils of web login. Important fixes from Microsoft.

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

• Breaches cost health care industry \$6 billion annually

Despite facing stricter privacy and security regulations, hospitals still are struggling to protect patient information, and breaches cost the health care industry \$6 billion annually, according to a new study. In the survey of 65 health care organizations, conducted by the Ponemon Institute and sponsored by data breach solutions provider ID Experts, 60 percent of respondents said they have suffered more than two breaches in the past two years.

The top three causes of breaches were unintentional employee action, lost or stolen computing devices and third-party accidents. The average number of lost or stolen records per breach was 1,769.

The survey found that breaches have cost the U.S. health care system \$12 billion over the past two years. The economic impact of a data breach was approximately \$2 million per organization over a two-year period. SC Magazine

Full Story :

http://www.scmagazineus.com/breaches-cost-health-care-industry-6-billion-annually/article/190493/?utm_source=feed

• Top 10 network vulnerabilities inside the network

Network World - Today's state-of-the-art network security appliances do a great job of keeping the cyber monsters from invading your business. But what do you do when the monster is actually inside the security perimeter? Unfortunately, all of the crosses, garlic, wooden stakes and silver bullets in the world have little effect on today's most nefarious cyber creatures. Here are the top 10 ways your network can be attacked from inside and what you can do to insure your business never has to perform an exorcism on your servers.

10 of the worst moments in network security history Computerworld

Full Story :

http://www.computerworld.com/s/article/9195458/Top_10_network_vulnerabilities_inside_the_network?source=rss

• Free Firefox add-ons detect Firesheep snooping

Every wireless-network user should know the perils of signing into a Web service over an unencrypted connection. Elinor Mills explains the perils of using open Wi-Fi networks in her InSecurity Complex blog.

The safest approach is to enter user IDs and passwords only when the page's address begins with "https://" and it has a lock icon at the top or bottom of the browser window. Otherwise a network snoop could monitor your actions without your knowledge. Note that the lock icon may have an exclamation mark even though the page address begins with "https:". This indicates that some of the current page's content could not be authenticated. Cnet Security

Full Story :

http://news.cnet.com/8301-13880_3-20022306-68.html?part=rss&subj=news&tag=2547-1_3-0-20

• Microsoft patches critical Outlook drive-by bug

Computerworld - Microsoft today patched 11 vulnerabilities, including one in Office that hackers will quickly exploit to launch drive-by attacks, said security experts.

As expected, Microsoft did not ship a fix for the flaw in Internet Explorer (IE) that criminals are currently using to hijack Windows PCs.

Of the 11 flaws addressed in three separate updates, only one was pegged as "critical," Microsoft's top ranking in its four-step scoring system. The remaining 10 were all marked "important," the second-highest rating. Computerworld

Full Story :

http://www.computerworld.com/s/article/9195719/Microsoft_patches_critical_Outlook_drive_by_bug?source=rss

• Get hacked and spill the beans, anonymously

A new Web site could help turn security breach guesswork into science.

Database breaches, social engineering attacks, and hacking incidents happen at companies every day, but very few end up being reported publicly. That's because organizations fear--and rightly so--damage to their reputation, public humiliation, and loss of customer confidence.

But this silent victim syndrome means that others can't learn from the missteps of victims and that the industry as a whole doesn't have a good grasp on the scope of the problem. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-20022451-245.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 12058 Outdated Windows Operating System no longer supported by Microsoft

A Host running an Old version of Windows that is No longer supported was found.

PCI Requirement: The ASV scan solution must be able to verify that the operating system is patched for these known exploits. The ASV scanning solution must also be able to determine the version of the operating system and whether it is an older version no longer supported by the vendor, in which case it must be marked as an automatic failure by the ASV.

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

References:

* MISC: Vendor site.

<http://www.microsoft.com>

* MISC: Windows Life Cycle Policy
<http://www.microsoft.com/windows/lifecycle/default.mspx>

CVE Reference:

• 13765 MySQL Database system detected

MySQL is a popular relational database management system (RDBMS) that runs as a server providing multi-user access to a number of databases. Many Web applications use MySQL as their backend database system.

An installation of MySQL was found.

PCI Requirement: The ASV scanning solution must be able to detect open access to databases from the Internet. This configuration is a violation of PCI DSS section 1.3.7, and must be marked as an automatic failure by the ASV. The ASV scanning solution must also be able to detect and report on known database exploits and vulnerabilities.

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

References:

- * MISC: Vendor site.
<http://www.mysql.com/>
- * MISC: MySQL Security Best Practices (Hardening MySQL Tips)
<http://www.greensql.net/publications/mysql-security-best-practices>
- * MISC: Ten MySQL Best Practices
<http://onlamp.com/pub/a/onlamp/2002/07/11/MySQLtips.html>

CVE Reference:

• 13768 Oracle Database system detected

The Oracle database is a relational database management system (RDBMS) produced and marketed by Oracle Corporation.

An installation of Oracle RDBMS was found.

PCI Requirement: The ASV scanning solution must be able to detect open access to databases from the Internet. This configuration is a violation of PCI DSS section 1.3.7, and must be marked as an automatic failure by the ASV. The ASV scanning solution must also be able to detect and report on known database exploits and vulnerabilities.

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

References:

- * MISC: Vendor site.
<http://www.oracle.com/index.html>
- * MISC: Oracle Security
<http://www.oracle.com/technetwork/topics/security/whatsnew/index.html>
- * MISC: Oracle Security papers
<http://www.petefinnigan.com/orasec.htm>

CVE Reference:

• 18993 PowerPoint Parsing Buffer Overflow Vulnerability (MS10-088/2293386) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft PowerPoint handles specially crafted PowerPoint 95 files. 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-2010-2924
<http://www.vupen.com/english/advisories/2010/2924>
- * BID: 44626
<http://www.securityfocus.com/bid/44626>
- * SECTRACK: 1024706
<http://securitytracker.com/alerts/2010/Nov/1024706.html>
- * MS: MS10-088
<http://www.microsoft.com/technet/security/Bulletin/MS10-088.mspx>

CVE Reference:

CVE-2010-2572 (cve.mitre.org, nvd.nist.gov)

• **18994 PowerPoint Integer Underflow Causes Heap Corruption Vulnerability (MS10-088/2293386) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft PowerPoint handles specially crafted PowerPoint files. 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-2010-2924
<http://www.vupen.com/english/advisories/2010/2924>
- * BID: 44628
<http://www.securityfocus.com/bid/44628>
- * SECTRACK: 1024706
<http://securitytracker.com/alerts/2010/Nov/1024706.html>
- * MS: MS10-088
<http://www.microsoft.com/technet/security/Bulletin/MS10-088.msp>

CVE Reference:

CVE-2010-2573 (cve.mitre.org, nvd.nist.gov)

• **18995 RTF Stack Buffer Overflow Vulnerability (MS10-087/2423930) (Remote File Checking)**

A remote code execution vulnerability exists in the way that affected Microsoft Office software parses specially crafted Rich Text Format (RTF) data. 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:

- * VUPEN: VUPEN/ADV-2010-2923
<http://www.vupen.com/english/advisories/2010/2923>
- * BID: 44652
<http://www.securityfocus.com/bid/44652>
- * SECTRACK: 1024705
<http://securitytracker.com/alerts/2010/Nov/1024705.html>
- * MS: MS10-087
<http://www.microsoft.com/technet/security/Bulletin/MS10-087.msp>

CVE Reference:

CVE-2010-3333 (cve.mitre.org, nvd.nist.gov)

• **18996 Office Art Drawing Records Vulnerability (MS10-087/2423930) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office software parses specially crafted Office files. 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:

- * VUPEN: VUPEN/ADV-2010-2923
<http://www.vupen.com/english/advisories/2010/2923>
- * BID: 44656
<http://www.securityfocus.com/bid/44656>
- * SECTRACK: 1024705
<http://securitytracker.com/alerts/2010/Nov/1024705.html>
- * MS: MS10-087
<http://www.microsoft.com/technet/security/Bulletin/MS10-087.msp>

CVE Reference:

CVE-2010-3334 (cve.mitre.org, nvd.nist.gov)

• **18997 Drawing Exception Handling Vulnerability (MS10-087/2423930) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office software parses specially crafted Office files. 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:

- * VUPEN: VUPEN/ADV-2010-2923
<http://www.vupen.com/english/advisories/2010/2923>
- * BID: 44659
<http://www.securityfocus.com/bid/44659>
- * SECTRACK: 1024705
<http://securitytracker.com/alerts/2010/Nov/1024705.html>
- * MS: MS10-087
<http://www.microsoft.com/technet/security/Bulletin/MS10-087.msp>

CVE Reference:

CVE-2010-3335 (cve.mitre.org, nvd.nist.gov)

• **18998 MSO Large SPID Read AV Vulnerability (MS10-087/2423930) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office software parses specially crafted Office files. 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:

- * VUPEN: VUPEN/ADV-2010-2923
<http://www.vupen.com/english/advisories/2010/2923>
- * BID: 44660
<http://www.securityfocus.com/bid/44660>
- * SECTRACK: 1024705
<http://securitytracker.com/alerts/2010/Nov/1024705.html>
- * MS: MS10-087
<http://www.microsoft.com/technet/security/Bulletin/MS10-087.msp>

CVE Reference:

CVE-2010-3336 (cve.mitre.org, nvd.nist.gov)

• **18999 Insecure Library Loading Vulnerability (MS10-087/2423930) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Office handles the loading of DLL files. 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:

- * VUPEN: VUPEN/ADV-2010-2923
<http://www.vupen.com/english/advisories/2010/2923>
- * BID: 42628
<http://www.securityfocus.com/bid/42628>
- * SECTRACK: 1024705
<http://securitytracker.com/alerts/2010/Nov/1024705.html>
- * MS: MS10-087
<http://www.microsoft.com/technet/security/Bulletin/MS10-087.msp>

CVE Reference:

New Vulnerabilities found this Week

- **CVE-2010-2572 Microsoft CVSS 2.0 Score = 9.3**

Buffer overflow in Microsoft PowerPoint 2002 SP3 and 2003 SP3 allows remote attackers to execute arbitrary code via a crafted PowerPoint 95 document, aka "PowerPoint Parsing Buffer Overflow Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-088.msp>

CVE Reference: [CVE-2010-2572](#)

- **CVE-2010-2573 Microsoft CVSS 2.0 Score = 9.3**

Integer underflow in Microsoft PowerPoint 2002 SP3 and 2003 SP3, PowerPoint Viewer SP2, and Office 2004 for Mac allows remote attackers to execute arbitrary code via a crafted PowerPoint document, aka "PowerPoint Integer Underflow Causes Heap Corruption Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-088.msp>

CVE Reference: [CVE-2010-2573](#)

- **CVE-2010-3333 Microsoft CVSS 2.0 Score = 9.3**

Stack-based buffer overflow in Microsoft Office XP SP3, Office 2003 SP3, Office 2007 SP2, Office 2010, Office 2004 and 2008 for Mac, Office for Mac 2011, and Open XML File Format Converter for Mac allows remote attackers to execute arbitrary code via crafted RTF data, aka "RTF Stack Buffer Overflow Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-087.msp>

CVE Reference: [CVE-2010-3333](#)

- **CVE-2010-3334 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office XP SP3, Office 2003 SP3, Office 2007 SP2, Office 2010, Office 2004 and 2008 for Mac, Office for Mac 2011, and Open XML File Format Converter for Mac allow remote attackers to execute arbitrary code via an Office document containing an Office Art Drawing record with crafted msofbtSp records and unspecified flags, which triggers memory corruption, aka "Office Art Drawing Records Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-087.msp>

CVE Reference: [CVE-2010-3334](#)

- **CVE-2010-3335 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office XP SP3, Office 2003 SP3, Office 2007 SP2, Office 2010, Office 2004 and 2008 for Mac, Office for Mac 2011, and Open XML File Format Converter for Mac allow remote attackers to execute arbitrary code via a crafted Office document that triggers memory corruption, aka "Drawing Exception Handling Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-087.msp>

CVE Reference: [CVE-2010-3335](#)

- **CVE-2010-3336 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office XP SP3, Office 2004 and 2008 for Mac, Office for Mac 2011, and Open XML File Format Converter for Mac allow remote attackers to execute arbitrary code via a crafted Office document that triggers memory corruption, aka "MSO Large SPID Read AV Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-087.msp>

CVE Reference: [CVE-2010-3336](#)

• **CVE-2010-3337 Microsoft CVSS 2.0 Score = 9.3**

Untrusted search path vulnerability in Microsoft Office 2007 SP2 and 2010 allows local users to gain privileges via a Trojan horse DLL in the current working directory, aka "Insecure Library Loading Vulnerability." NOTE: this might overlap CVE-2010-3141 and CVE-2010-3142. Per: <http://www.microsoft.com/technet/security/Bulletin/MS10-087.msp> 'FAQ for Insecure Library Loading Vulnerability - CVE-2010-3337: This is a remote code execution vulnerability.'

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-087.msp>

CVE Reference: [CVE-2010-3337](#)

• **CVE-2010-2732 Microsoft CVSS 2.0 Score = 5.8**

Open redirect vulnerability in the web interface in Microsoft Forefront Unified Access Gateway (UAG) 2010 Gold, 2010 Update 1, and 2010 Update 2 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors, aka "UAG Redirection Spoofing Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS10-089.msp>

CVE Reference: [CVE-2010-2732](#)

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@securescout.net