

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

[Messenger Service Vulnerability Scanner](#) - The S4 Messenger Service 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 Microsoft Windows Messenger Service flaw (MS03-043).

Download Here:

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

This Week in Review

The British investigates cyberattacks. CEOs need to be more security conscious. Can the internet help you through tough times? Living robots?

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

• Probe into cyberattacks stretches around the globe

IDG News Service - British authorities have launched an investigation into the recent cyberattacks that crippled Web sites in the U.S. and South Korea, as the trail to find the perpetrators stretches around the world.

On Tuesday, the Vietnamese security vendor Bach Khoa Internetwork Security (Bkis) said it had identified a master command-and-control server used to coordinate the denial-of-service (DDoS) attacks, which took down major U.S. and South Korean government Web sites.

A command-and-control server is used to distribute instructions to zombie PCs, which form a botnet that can be used to bombard Web sites with traffic, rendering the sites useless. The server was on an IP (Internet Protocol) address used by Global Digital Broadcast, an IP TV technology company based in Brighton, England, according to Bkis.

Computerworld

Full Story :

http://www.computerworld.com/s/article/9135532/Probe_into_cyberattacks_stretches_around_the_globe?source=rss

• CEOs underestimate security risks, survey finds

Computerworld - Compared to other key corporate executives, CEOs appear to underestimate the IT security risks faced by their own organizations, according to a survey of C-level executives released today by the Ponemon Institute.

The Ponemon survey (download PDF) of 213 CEOs, CIOs, COOs and other senior executives reveals what appears to be a perception gap concerning information security issues between CEOs and other senior managers. For instance, 48% of CEOs surveyed said they believe hackers rarely try to access corporate data. On the other hand, some 53% of other C-level executives believe that their company's data is under attack on a daily or even hourly basis.

The survey also found that the top executives were less aware of specific security incidents at their companies than other C-level executives, and are more confident that data breaches can be easily avoided. Computerworld

Full Story :

http://www.computerworld.com/s/article/9135569/CEOs_underestimate_security_risks_survey_finds?source=rss_se

• Americans relying on Internet to fight tough times, report says

If you find yourself in front of your computer screen looking to understand the recession and find ways to deal with it, you're not alone.

According to a report released Wednesday by the Pew Research Center, some 69 percent of American adults, or 88 percent of U.S. Internet users, have gone online in the past year for reasons related to the recession. The study says they either are trying to get help with personal economic issues or gather information about the origins of national economic problems and solutions to those difficulties.

Americans look to the Internet to cope with the recession. Cnet Security

Full Story :

http://news.cnet.com/8301-1023_3-10287679-93.html?part=rss&subj=news&tag=2547-1_3-0-20

• Dawn of the corpse-eating robots?

In the future, we will need robots to do our dirty work.

In the future, we will need robots to do our clean work, too.

So in the future, we will need our robots to live, like farmers in centuries gone by, off the fat of the land. Cnet Security

Full Story :

http://news.cnet.com/8301-17852_3-10287597-71.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 14755 Mozilla Firefox error within the verification of certain signatures in NSS library (CVE-2006-5462) (Remote File Checking)

A vulnerability has been reported in Mozilla Network Security Services (NSS), which potentially can be exploited by malicious people to bypass certain security restrictions.

The weakness has been fixed in version 1.5.0.8.

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

References:

* MISC:

<http://www.mozilla.org/security/announce/2006/mfsa2006-60.html>

* MISC:

https://bugzilla.mozilla.org/show_bug.cgi?id=356215

* CONFIRM:

<http://www.mozilla.org/security/announce/2006/mfsa2006-66.html>

* CONFIRM:

<http://support.avaya.com/elmodocs2/security/ASA-2006-246.htm>

* DEBIAN: DSA-1224

<http://www.debian.org/security/2006/dsa-1224>

* DEBIAN: DSA-1225

<http://www.debian.org/security/2006/dsa-1225>

* DEBIAN: DSA-1227

<http://www.debian.org/security/2006/dsa-1227>
* GENTOO: GLSA-200612-06
<http://security.gentoo.org/glsa/glsa-200612-06.xml>
* GENTOO: GLSA-200612-07
<http://security.gentoo.org/glsa/glsa-200612-07.xml>
* GENTOO: GLSA-200612-08
<http://security.gentoo.org/glsa/glsa-200612-08.xml>
* HP: HPSBUX02153
<http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=c00771742>
* MANDRIVA: MDKSA-2006:205
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:205>
* MANDRIVA: MDKSA-2006:206
<http://www.mandriva.com/security/advisories?name=MDKSA-2006:206>
* REDHAT: RHSA-2006:0733
<http://rhn.redhat.com/errata/RHSA-2006-0733.html>
* REDHAT: RHSA-2006:0734
<http://rhn.redhat.com/errata/RHSA-2006-0734.html>
* REDHAT: RHSA-2006:0735
<http://rhn.redhat.com/errata/RHSA-2006-0735.html>
* SGI: 20061101-01-P
ftp://patches.sgi.com/support/free/security/advisories/20061101-01-P
* SUNALERT: 102781
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102781-1>
* SUSE: SUSE-SA:2006:068
http://www.novell.com/linux/security/advisories/2006_68_mozilla.html
* UBUNTU: USN-381-1
<http://www.ubuntu.com/usn/usn-381-1>
* UBUNTU: USN-382-1
<http://www.ubuntu.com/usn/usn-382-1>
* CERT: TA06-312A
<http://www.us-cert.gov/cas/techalerts/TA06-312A.html>
* CERT-VN: VU#335392
<http://www.kb.cert.org/vuls/id/335392>
* VUPEN: ADV-2006-4387
<http://www.frsirt.com/english/advisories/2006/4387>
* VUPEN: ADV-2007-0293
<http://www.frsirt.com/english/advisories/2007/0293>
* VUPEN: ADV-2007-1198
<http://www.frsirt.com/english/advisories/2007/1198>
* VUPEN: ADV-2006-3748
<http://www.frsirt.com/english/advisories/2006/3748>
* VUPEN: ADV-2008-0083
<http://www.frsirt.com/english/advisories/2008/0083>
* SECTRACK: 1017180
<http://securitytracker.com/id?1017180>
* SECTRACK: 1017181
<http://securitytracker.com/id?1017181>
* SECTRACK: 1017182
<http://securitytracker.com/id?1017182>
* SECUNIA: 22722
<http://secunia.com/advisories/22722>
* SECUNIA: 22770
<http://secunia.com/advisories/22770>
* SECUNIA: 22727
<http://secunia.com/advisories/22727>
* SECUNIA: 22737
<http://secunia.com/advisories/22737>
* SECUNIA: 22763
<http://secunia.com/advisories/22763>
* SECUNIA: 22817
<http://secunia.com/advisories/22817>
* SECUNIA: 22929
<http://secunia.com/advisories/22929>
* SECUNIA: 22965
<http://secunia.com/advisories/22965>
* SECUNIA: 22980
<http://secunia.com/advisories/22980>
* SECUNIA: 23009
<http://secunia.com/advisories/23009>

* SECUNIA: 23013
<http://secunia.com/advisories/23013>
* SECUNIA: 23197
<http://secunia.com/advisories/23197>
* SECUNIA: 23202
<http://secunia.com/advisories/23202>
* SECUNIA: 23235
<http://secunia.com/advisories/23235>
* SECUNIA: 23263
<http://secunia.com/advisories/23263>
* SECUNIA: 23287
<http://secunia.com/advisories/23287>
* SECUNIA: 23297
<http://secunia.com/advisories/23297>
* SECUNIA: 23883
<http://secunia.com/advisories/23883>
* SECUNIA: 22815
<http://secunia.com/advisories/22815>
* SECUNIA: 24711
<http://secunia.com/advisories/24711>
* SECUNIA: 22066
<http://secunia.com/advisories/22066>
* XF: mozilla-nss-security-bypass(30098)
<http://xforce.iss.net/xforce/xfdb/30098>

CVE Reference:

CVE-2006-5462 (cve.mitre.org, nvd.nist.gov)

• 18437 Microsoft Word Mail Merge Vulnerability (MS06-060/924554) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Word, and could be exploited when Word opens a specially crafted mail merge file. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious web site. Viewing or previewing a malformed e-mail message in an affected version of Outlook could not lead to exploitation of this vulnerability. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution.

If a user were 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 affected than users who operate with administrative user rights.

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

References:

* HP: HPSBST02161
<http://www.securityfocus.com/archive/1/archive/1/449179/100/0/threaded>
* MS: MS06-060
<http://www.microsoft.com/technet/security/Bulletin/MS06-060.mspx>
* CERT-VN: VU#921300
<http://www.kb.cert.org/vuls/id/921300>
* BID: 20358
<http://www.securityfocus.com/bid/20358>
* VUPEN: ADV-2006-3979
<http://www.frsirt.com/english/advisories/2006/3979>
* OVAL: oval:org.mitre.oval:def:51
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:51>
* SECTRACK: 1017032
<http://securitytracker.com/id?1017032>

CVE Reference:

CVE-2006-3651 (cve.mitre.org, nvd.nist.gov)

• 18438 Microsoft Word Malformed Stack Vulnerability (MS06-060/924554) (Remote File Checking)

A remote code execution vulnerability exists in Microsoft Word, and could be exploited when Word opens a specially crafted file. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious web site. Viewing or previewing a malformed e-mail message in an affected version of Outlook could not lead to exploitation of this vulnerability. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution.

If a user were 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 affected than users who operate with administrative user rights.

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

References:

- * BUGTRAQ: 20060906 Microsoft confirmed Word 0-day vulnerability
<http://www.securityfocus.com/archive/1/archive/1/445381/100/0/threaded>
- * BUGTRAQ: 20060906 Re: Microsoft Word 0-day Vulnerability (September) FAQ document available
<http://www.securityfocus.com/archive/1/archive/1/445285/100/0/threaded>
- * BUGTRAQ: 20060905 Microsoft Word 0-day Vulnerability (September) FAQ document available
<http://www.securityfocus.com/archive/1/archive/1/445162/100/100/threaded>
- * MISC:
<http://blogs.securiteam.com/?p=586>
- * MISC:
<http://isc.sans.org/diary.php?storyid=1669>
- * MISC:
http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-090219-2855-99
- * MISC:
http://vil.mcafeesecurity.com/vil/content/v_119055.htm
- * CONFIRM:
<http://www.microsoft.com/technet/security/advisory/925059.mspx>
- * HP: HPSBST02161
<http://www.securityfocus.com/archive/1/archive/1/449179/100/0/threaded>
- * MS: MS06-060
<http://www.microsoft.com/technet/security/Bulletin/MS06-060.mspx>
- * MSKB: Q925059
<http://support.microsoft.com/kb/925059>
- * CERT-VN: VU#806548
<http://www.kb.cert.org/vuls/id/806548>
- * BID: 19835
<http://www.securityfocus.com/bid/19835>
- * VUPEN: ADV-2006-3448
<http://www.frsirt.com/english/advisories/2006/3448>
- * OSVDB: 28539
<http://www.osvdb.org/28539>
- * OVAL: oval:org.mitre.oval:def:578
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:578>
- * SECTRACK: 1016787
<http://securitytracker.com/id?1016787>
- * SECUNIA: 21735
<http://secunia.com/advisories/21735>
- * XF: ms-word-code-execution(28775)
<http://xforce.iss.net/xforce/xfdb/28775>

CVE Reference:

CVE-2006-4534 (cve.mitre.org, nvd.nist.gov)

• 18439 Microsoft Word for Mac Vulnerability (MS06-060/924554) (Remote File Checking)

A remote code execution vulnerability exists in Word for Mac. An attacker could exploit this vulnerability when Word for Mac parses a specially crafted file that contains a malformed string. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious web site. Viewing or previewing a malformed e-mail message in Outlook could not lead to exploitation of this vulnerability. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution.

If a user were 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 affected than users who operate with administrative user rights.

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

References:

- * HP: HPSBST02161
<http://www.securityfocus.com/archive/1/archive/1/449179/100/0/threaded>
- * MS: MS06-060

<http://www.microsoft.com/technet/security/Bulletin/MS06-060.msp>

* BID: 20387

<http://www.securityfocus.com/bid/20387>

* VUPEN: ADV-2006-3979

<http://www.frsirt.com/english/advisories/2006/3979>

* OSVDB: 29442

<http://www.osvdb.org/29442>

* SECTRACK: 1017032

<http://securitytracker.com/id?1017032>

CVE Reference:

CVE-2006-4693 (cve.mitre.org, nvd.nist.gov)

• 18440 DirectX NULL Byte Overwrite Vulnerability (MS09-028/971633) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft DirectShow parses QuickTime media files. This vulnerability could allow code execution if a user opened a specially crafted QuickTime 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:

* MISC:

<http://isc.sans.org/diary.html?storyid=6481>

* CONFIRM:

<http://blogs.technet.com/msrc/archive/2009/05/28/microsoft-security-advisory-971778-vulnerability-in-microsoft-directshow>

* CONFIRM:

<http://blogs.technet.com/srd/archive/2009/05/28/new-vulnerability-in-quicktime-parsing.aspx>

* CONFIRM:

<http://www.microsoft.com/technet/security/advisory/971778.msp>

* BID: 35139

<http://www.securityfocus.com/bid/35139>

* OSVDB: 54797

<http://osvdb.org/54797>

* SECTRACK: 1022299

<http://www.securitytracker.com/id?1022299>

* SECUNIA: 35268

<http://secunia.com/advisories/35268>

* VUPEN: ADV-2009-1445

<http://www.vupen.com/english/advisories/2009/1445>

CVE Reference:

CVE-2009-1537 (cve.mitre.org, nvd.nist.gov)

• 18441 DirectX Pointer Validation Vulnerability (MS09-028/971633) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft DirectShow validates certain values when updating a pointer. This vulnerability could allow code execution if a user opened a specially crafted QuickTime 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: MS09-028

<http://www.microsoft.com/technet/security/bulletin/MS09-028.msp>

* BID: Microsoft DirectX DirectShow Pointer Validation Remote Code Execution Vulnerability

<http://www.securityfocus.com/bid/35600>

CVE Reference:

CVE-2009-1538 (cve.mitre.org, nvd.nist.gov)

• 18442 DirectX Size Validation Vulnerability (MS09-028/971633) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft DirectShow validates specific fields in QuickTime media files. This vulnerability could allow code execution if a user opened a specially crafted QuickTime 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: MS09-028

<http://www.microsoft.com/technet/security/bulletin/MS09-028.msp>

* BID: Microsoft DirectX DirectShow Length Record Remote Code Execution Vulnerability

<http://www.securityfocus.com/bid/35616>

CVE Reference:

CVE-2009-1539 (cve.mitre.org, nvd.nist.gov)

• **18443 Embedded OpenType Font Heap Overflow Vulnerability (MS09-029/961371) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Windows Embedded OpenType (EOT) font technology parses data records in specially crafted embedded fonts. 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: MS09-029

<http://www.microsoft.com/technet/security/bulletin/MS09-029.msp>

* BID: Microsoft Windows Embedded OpenType Font Engine Heap Overflow Vulnerability

<http://www.securityfocus.com/bid/35186>

CVE Reference:

CVE-2009-0231 (cve.mitre.org, nvd.nist.gov)

• **18444 Embedded OpenType Font Integer Overflow Vulnerability (MS09-029/961371) (Remote File Checking)**

A remote code execution vulnerability exists in the way that Microsoft Windows Embedded OpenType (EOT) font technology parses name tables in specially crafted embedded fonts. 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: MS09-029

<http://www.microsoft.com/technet/security/bulletin/MS09-029.msp>

* BID: Microsoft Windows Embedded OpenType Font Engine Integer Overflow Vulnerability

<http://www.securityfocus.com/bid/35187>

CVE Reference:

CVE-2009-0232 (cve.mitre.org, nvd.nist.gov)

• **18445 Microsoft ISA Server 2006 Radius OTP Bypass Vulnerability (MS09-031/970953) (Remote File Checking)**

An elevation of privilege vulnerability exists in ISA Server 2006 authentication when configured with Radius OTP. The vulnerability could allow an unauthenticated user access to any Web published resource. With knowledge of administrator account usernames, an attacker who successfully exploited this vulnerability could take complete control of systems relying on the ISA Server 2006 Web publishing rules for authentication. 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: MS09-031

<http://www.microsoft.com/technet/security/bulletin/ms09-031.msp>

* BID: Microsoft ISA Server Radius OTP Authentication Bypass Vulnerability

<http://www.securityfocus.com/bid/35631>

CVE Reference:

CVE-2009-1135 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-1136 Microsoft CVSS 2.0 Score = 10.0

The Microsoft Office Web Components Spreadsheet ActiveX control (aka OWC10 or OWC11), as distributed in Office XP SP3 and Office 2003 SP3, Office XP Web Components SP3, Office 2003 Web Components SP3, Office 2003 Web Components for the 2007 Microsoft Office system SP1, Internet Security and Acceleration (ISA) Server 2004 SP3 and 2006 Gold and SP1, and Office Small Business Accounting 2006, when used in Internet Explorer, allows remote attackers to execute arbitrary code via a crafted call to the msDataSourceObject method.

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

References:

MISC: <http://xeye.us/blog/2009/07/one-0day/>

CONFIRM: <http://www.microsoft.com/technet/security/advisory/973472.msp>

MISC:

http://trac.metasploit.com/browser/framework3/trunk/modules/exploits/windows/browser/owc_spreadsheet_msdsob.rb

MISC: <http://isc.sans.org/diary.html?storyid=6778>

CONFIRM:

<http://blogs.technet.com/srd/archive/2009/07/13/more-information-about-the-office-web-components-activex-vulnerability.aspx>

CONFIRM: <http://blogs.technet.com/msrc/archive/2009/07/13/microsoft-security-advisory-973472-released.aspx>

CVE Reference: [CVE-2009-1136](http://cve.mitre.org/cve/2009/1136)

• CVE-2009-1542 Microsoft CVSS 2.0 Score = 10.0

The Virtual Machine Monitor (VMM) in Microsoft Virtual PC 2004 SP1, 2007, and 2007 SP1, and Microsoft Virtual Server 2005 R2 SP1, does not enforce CPU privilege-level requirements for all machine instructions, which allows guest OS users to execute arbitrary kernel-mode code and gain privileges within the guest OS via a crafted application, aka "Virtual PC and Virtual Server Privileged Instruction Decoding Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-033.msp>

CVE Reference: [CVE-2009-1542](http://cve.mitre.org/cve/2009/1542)

• CVE-2009-0231 Microsoft CVSS 2.0 Score = 9.3

Heap-based buffer overflow in the Embedded OpenType (EOT) Font Engine in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a crafted name table in a data record, aka "Embedded OpenType Font Heap Overflow Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-029.msp>

CVE Reference: [CVE-2009-0231](http://cve.mitre.org/cve/2009/0231)

• CVE-2009-0232 Microsoft CVSS 2.0 Score = 9.3

Integer overflow in the Embedded OpenType (EOT) Font Engine in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a crafted name table, aka "Embedded OpenType Font Integer Overflow Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-029.msp>

CVE Reference: [CVE-2009-0232](#)

• **CVE-2009-0566 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Office Publisher 2007 SP1 does not properly calculate object handler data for Publisher files, which allows remote attackers to execute arbitrary code via a crafted file in a legacy format that triggers memory corruption, aka "Pointer Dereference Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-030.msp>

CVE Reference: [CVE-2009-0566](#)

• **CVE-2009-1538 Microsoft CVSS 2.0 Score = 9.3**

The QuickTime Movie Parser Filter in quartz.dll in DirectShow in Microsoft DirectX 7.0 through 9.0c on Windows 2000 SP4, Windows XP SP2 and SP3, and Windows Server 2003 SP2 performs updates to pointers without properly validating unspecified data values, which allows remote attackers to execute arbitrary code via a crafted QuickTime media file, aka "DirectX Pointer Validation Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-028.msp>

CVE Reference: [CVE-2009-1538](#)

• **CVE-2009-1539 Microsoft CVSS 2.0 Score = 9.3**

The QuickTime Movie Parser Filter in quartz.dll in DirectShow in Microsoft DirectX 7.0 through 9.0c on Windows 2000 SP4, Windows XP SP2 and SP3, and Windows Server 2003 SP2 does not properly validate unspecified size fields in QuickTime media files, which allows remote attackers to execute arbitrary code via a crafted file, aka "DirectX Size Validation Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-028.msp>

CVE Reference: [CVE-2009-1539](#)

• **CVE-2009-1135 Microsoft CVSS 2.0 Score = 9.0**

Microsoft Internet Security and Acceleration (ISA) Server 2006 Gold and SP1, when Radius OTP is enabled, uses the HTTP-Basic authentication method, which allows remote attackers to gain the privileges of an arbitrary account, and access published web pages, via vectors involving attempted access to a network resource behind the ISA Server, aka "Radius OTP Bypass Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS09-031.msp>

CVE Reference: [CVE-2009-1135](#)

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