

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).

The National Vulnerability Database (NVD) part of the National Institute of Standards and Technology (NIST) has recognized netVigilance for its detailed feedback on the NVD CVSS v2 scores. See <http://www.netvigilance.com/press6-16-08>

This Week in Review

Attacks against insurance market increasingly professional. Corporate networks still lacking security. Resistance against new Swedish law. UK government tries to regain peoples confidence.

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

- ❖ Lloyd's faces up to threat of e-crime

Lloyd's of London tackles 60 severe attacks each day by upping defences and aligning IT resources

The growing trend of organised gangs turning to e-crime has been confirmed by Lloyd's of London, whose networks have been bombarded by structured and competent attacks.

Over the past 12 months the world's largest insurance market has found that attacks on its systems have become more professional.

"We have noticed a drop off in what I would term 'the enthusiastic hacker', the academics who simply want to break through your firewall," said Peter Hambling, chief information officer (CIO) at Lloyd's of London.

Computeractive

Full Story :

<http://www.computeractive.co.uk/computing/analysis/2219887/lloyd-faces-threat-crime>

❖ Most corporate networks vulnerable to cyberattacks

Eighty-one percent of corporate end points failed basic security checks in a wide ranging global survey by security solutions and services provider Sophos.

According to the security firm's initial findings from the Sophos Endpoint Assessment Test, these checks established the ability of enterprises to properly assess and control baseline endpoint security requirements such as updated patches, enabled firewalls and current anti-malware signatures updates.

Don't Miss! Read the latest WhitePaper - Troubleshooting Remote Site Networks - Best Practices

"Machines that fail such a test represent 'low hanging fruit' for cybercriminals and a real danger to their corporate networks," said Jim Dowling, director of sales for Asia, Sophos.

networkworld

Full Story :

<http://www.networkworld.com/news/2008/062308-most-corporate-networks-vulnerable-to.html?t51hb>

❖ Pirate Bay uses encryption to scupper new law

'We want Sweden to be banned from the internet'

Controversial BitTorrent site The Pirate Bay is adding encryption to its website in order to counter a new Swedish law that allows wiretapping of internet and phone traffic.

"Many people have asked me what we're planning to do, and the answer is 'A lot!'" spokesman and co-founder Peter Sunde wrote in his blog. "This week we're going to add SSL [secure sockets layer] to The Pirate Bay".

He also has a message for international ISPs: "We want Sweden to be banned from the internet. The ISPs need to block Sweden in order to protect their own customers' integrity since everything they do on Swedish ISPs' networks will be logged and searched."

PC Advisor

Full Story :

<http://www.pcadvisor.co.uk/news/index.cfm?newsid=13506>

❖ UK.gov calls on white hat hackers to spot data leaks

HMRC debacle to foster 'culture change', says Cabinet Office

The civil service's systems will be subjected to new attacks by independent white hat hackers in a bid to spot weaknesses in government data handling before catastrophic losses occur, it was announced today.

The white hat programme is one of a suite of targets, training and scrutiny measures that Cabinet Secretary Gus O'Donnell hopes will bring about a "culture change" across the civil service and restore public faith in the government's competence in handling sensitive data.

He said: "The risk we must counter is that citizens and business lose trust in the Government to handle their data effectively. It would be foolish not to acknowledge that the lapses in data security have affected this confidence."

The Register

Full Story :

http://www.theregister.co.uk/2008/06/25/cabinet_office_data_handling_report/

New Vulnerabilities Tested in SecureScout

- **16965 QuickTime parsing of 'crgn' atoms may result in a heap buffer overflow (Remote File Checking)**

An issue in QuickTime's parsing of 'crgn' atoms may result in a heap buffer overflow. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.4.5.

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

References:

* BUGTRAQ: 20080403 ZDI-08-015: Apple QuickTime Clipping Region Heap Overflow Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/490460/100/0/threaded>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-08-015>

* CONFIRM:

<http://support.apple.com/kb/HT1241>

* CERT: TA08-094A

<http://www.us-cert.gov/cas/techalerts/TA08-094A.html>

* BID: 28583

<http://www.securityfocus.com/bid/28583>

* FRSIRT: ADV-2008-1078

<http://www.frsirt.com/english/advisories/2008/1078>

* SECTRACK: 1019761

<http://securitytracker.com/id?1019761>

* SECUNIA: 29650

<http://secunia.com/advisories/29650>

* XF: quicktime-crgn-bo(41607)

<http://xforce.iss.net/xforce/xfdb/41607>

CVE Reference:

CVE-2008-1017 (cve.mitre.org, nvd.nist.gov)

• 16966 QuickTime parsing of 'chan' atoms may result in a heap buffer overflow (Remote File Checking)

An issue in QuickTime's parsing of 'chan' atoms may result in a heap buffer overflow. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.4.5.

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

References:

* BUGTRAQ: 20080403 ZDI-08-016: Apple QuickTime MP4A Atom Parsing Heap Corruption Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/490467/100/0/threaded>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-08-016>

* CONFIRM:

<http://support.apple.com/kb/HT1241>

* CERT: TA08-094A

<http://www.us-cert.gov/cas/techalerts/TA08-094A.html>

* BID: 28583

<http://www.securityfocus.com/bid/28583>

* FRSIRT: ADV-2008-1078

<http://www.frsirt.com/english/advisories/2008/1078>

* SECTRACK: 1019762

<http://securitytracker.com/id?1019762>

* SECUNIA: 29650

<http://secunia.com/advisories/29650>

* XF: quicktime-chan-bo(41606)

<http://xforce.iss.net/xforce/xfdb/41606>

CVE Reference:

CVE-2008-1018 (cve.mitre.org, nvd.nist.gov)

• 16967 QuickTime handling of PICT records may result in a heap buffer overflow (Remote File Checking)

An issue in QuickTime's handling of PICT records may result in a heap buffer overflow. Viewing a maliciously crafted PICT image file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.4.5.

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

References:

* BUGTRAQ: 20080403 ZDI-08-014: Apple Quicktime Multiple Opcode Memory Corruption Vulnerabilities

<http://www.securityfocus.com/archive/1/archive/1/490459/100/0/threaded>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-08-014>

* CONFIRM:

<http://support.apple.com/kb/HT1241>

* CERT: TA08-094A

<http://www.us-cert.gov/cas/techalerts/TA08-094A.html>

* BID: 28583

<http://www.securityfocus.com/bid/28583>

* FRSIRT: ADV-2008-1078

<http://www.frsirt.com/english/advisories/2008/1078>

* SECTRACK: 1019763

<http://securitytracker.com/id?1019763>

* SECUNIA: 29650

<http://secunia.com/advisories/29650>

* XF: quicktime-pict-records-bo(41609)

<http://xforce.iss.net/xforce/xfdb/41609>

CVE Reference:

CVE-2008-1019 (cve.mitre.org, nvd.nist.gov)

• 16968 QuickTime handling of error messages during PICT images processing may result in a heap buffer overflow (Remote File Checking)

An issue in QuickTime's handling of error messages during PICT images processing may result in a heap buffer overflow. Viewing a maliciously crafted PICT image may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.4.5.

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

References:

* BUGTRAQ: 20080403 ZDI-08-014: Apple Quicktime Multiple Opcode Memory Corruption Vulnerabilities

<http://www.securityfocus.com/archive/1/archive/1/490459/100/0/threaded>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-08-014>

* CONFIRM:

<http://support.apple.com/kb/HT1241>

* CERT: TA08-094A

<http://www.us-cert.gov/cas/techalerts/TA08-094A.html>

* BID: 28583

<http://www.securityfocus.com/bid/28583>

* FRSIRT: ADV-2008-1078

<http://www.frsirt.com/english/advisories/2008/1078>

* SECTRACK: 1019763

<http://securitytracker.com/id?1019763>

* SECUNIA: 29650

<http://secunia.com/advisories/29650>

* XF: quicktime-pict-records-bo(41609)

<http://xforce.iss.net/xforce/xfdb/41609>

CVE Reference:

CVE-2008-1019 (cve.mitre.org, nvd.nist.gov)

• 16969 QuickTime handling of Animation codec content may result in a heap buffer overflow (Remote File Checking)

An issue in QuickTime's handling of Animation codec content may result in a heap buffer overflow. Viewing a maliciously crafted movie file with Animation codec content may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.4.5.

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

References:

* BUGTRAQ: 20080403 ZDI-08-018: Apple QuickTime Run Length Encoding Heap Overflow Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/490462/100/0/threaded>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-08-018>

* CONFIRM:

<http://support.apple.com/kb/HT1241>

* CERT: TA08-094A

<http://www.us-cert.gov/cas/techalerts/TA08-094A.html>

* BID: 28583

<http://www.securityfocus.com/bid/28583>

* FRSIRT: ADV-2008-1078

<http://www.frsirt.com/english/advisories/2008/1078>

* SECTRACK: 1019765

<http://securitytracker.com/id?1019765>

* SECUNIA: 29650

<http://secunia.com/advisories/29650>

* XF: quicktime-animation-codec-bo(41612)

<http://xforce.iss.net/xforce/xfdb/41612>

CVE Reference:

CVE-2008-1021 (cve.mitre.org, nvd.nist.gov)

- **16970 QuickTime parsing of 'obji' atoms may result in a stack buffer overflow (Remote File Checking)**

An issue in QuickTime's parsing of 'obji' atoms may result in a stack buffer overflow. Viewing a maliciously crafted QuickTime VR movie file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.4.5.

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

References:

* BUGTRAQ: 20080403 ZDI-08-019: Apple QuickTime Malformed VR obji Atom Parsing Memory Corruption Vulnerability

<http://www.securityfocus.com/archive/1/archive/1/490461/100/0/threaded>

* MISC:

<http://www.zerodayinitiative.com/advisories/ZDI-08-019>

* CONFIRM:

<http://support.apple.com/kb/HT1241>

* CERT: TA08-094A

<http://www.us-cert.gov/cas/techalerts/TA08-094A.html>

* BID: 28583

<http://www.securityfocus.com/bid/28583>

* FRSIRT: ADV-2008-1078

<http://www.frsirt.com/english/advisories/2008/1078>

* SECTRACK: 1019766

<http://securitytracker.com/id?1019766>

* SECUNIA: 29650

<http://secunia.com/advisories/29650>

* XF: quicktime-obji-atoms-bo(41613)

<http://xforce.iss.net/xforce/xfdb/41613>

CVE Reference:

CVE-2008-1022 (cve.mitre.org, nvd.nist.gov)

• 16971 QuickTime parsing of the Clip opcode may result in a heap buffer overflow (Remote File Checking)

An issue in QuickTime's parsing of the Clip opcode may result in a heap buffer overflow. Viewing a maliciously crafted PICT image file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.4.5.

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

References:

* CONFIRM:

<http://support.apple.com/kb/HT1241>

* CERT: TA08-094A

<http://www.us-cert.gov/cas/techalerts/TA08-094A.html>

* BID: 28583

<http://www.securityfocus.com/bid/28583>

* FRSIRT: ADV-2008-1078

<http://www.frsirt.com/english/advisories/2008/1078>

* SECTRACK: 1019767

<http://securitytracker.com/id?1019767>

* SECUNIA: 29650

<http://secunia.com/advisories/29650>

* XF: quicktime-clip-opcodes-bo(41615)

<http://xforce.iss.net/xforce/xfdb/41615>

CVE Reference:

CVE-2008-1023 (cve.mitre.org, nvd.nist.gov)

• **16972 QuickTime parsing of 'ftyp' atoms may result in memory corruption (Remote File Checking)**

An issue in QuickTime's parsing of 'ftyp' atoms may result in memory corruption. Viewing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution.

The issue has been fixed in version 7.4.5.

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

References:

* CONFIRM:

<http://support.apple.com/kb/HT1241>

* CERT: TA08-094A

<http://www.us-cert.gov/cas/techalerts/TA08-094A.html>

* BID: 28583

<http://www.securityfocus.com/bid/28583>

* FRSIRT: ADV-2008-1078

<http://www.frsirt.com/english/advisories/2008/1078>

* SECTRACK: 1019767

<http://securitytracker.com/id?1019767>

* SECUNIA: 29650

<http://secunia.com/advisories/29650>

* XF: quicktime-clip-opcodes-bo(41615)

<http://xforce.iss.net/xforce/xfdb/41615>

CVE Reference:

CVE-2008-1023 (cve.mitre.org, nvd.nist.gov)

• **16973 QuickTime cross-zone scripting vulnerability (Remote File Checking)**

A cross-zone scripting vulnerability in Apple Quicktime 3 to 7.1.3 allows remote user-assisted attackers to execute arbitrary code and list filesystem contents via a QuickTime movie (.MOV) with an HREF Track (HREFTrack) that contains an automatic action tag with a local URI, which is executed in a local zone during preview, as exploited by a MySpace worm.

The issue has been fixed in version 7.1.5.

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

References:

* MISC:

<http://projects.info-pull.com/moab/MOAB-03-01-2007.html>

* MISC:

<http://www.gnucitizen.org/blog/backdooring-quicktime-movies/>

* APPLE: APPLE-SA-2007-03-05

<http://lists.apple.com/archives/Security-announce/2007/Mar/msg00000.html>

* CONFIRM:

<http://docs.info.apple.com/article.html?artnum=305149>

* CERT-VN: VU#304064

<http://www.kb.cert.org/vuls/id/304064>

CVE Reference:

CVE-2007-0059 (cve.mitre.org, nvd.nist.gov)

• 16974 QuickTime QuickTime Media Link (QTL) file, arbitrary code execution vulnerability (Remote File Checking)

Apple QuickTime 7.1.3 Player and Plug-In allow remote attackers to execute arbitrary JavaScript code and possibly conduct other attacks via a QuickTime Media Link (QTL) file with an embed XML element and a qtnext parameter that identifies resources outside of the original domain. NOTE: as of 20070912, this issue has been demonstrated by using instances of Components.interfaces.nsILocalFile and Components.interfaces.nsIProcess to execute arbitrary local files within Firefox and possibly Internet Explorer.

The issue has been fixed in version 7.1.5.

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

References:

* BUGTRAQ: 20060920 Backdooring MP3 files (plus QuickTime issues and Cross-context Scripting)

<http://www.securityfocus.com/archive/1/archive/1/446750/100/0/threaded>

* BUGTRAQ: 20061207 New MySpace worm could be on its way

<http://www.securityfocus.com/archive/1/archive/1/453756/100/0/threaded>

* BUGTRAQ: 20070912 0DAY: QuickTime pwns Firefox

<http://www.securityfocus.com/archive/1/archive/1/479179/100/0/threaded>

* MISC:

<http://www.gnucitizen.org/blog/backdooring-mp3-files/>

* MISC:

<http://www.gnucitizen.org/blog/myspace-quicktime-worm-follow-up>

* MISC:

<http://www.gnucitizen.org/blog/0day-quicktime-pwns-firefox>

* CONFIRM:

<http://docs.info.apple.com/article.html?artnum=305149>

* APPLE: APPLE-SA-2007-03-05

<http://lists.apple.com/archives/Security-announce/2007/Mar/msg00000.html>

* CERT-VN: VU#751808

<http://www.kb.cert.org/vuls/id/751808>

* BID: 20138

<http://www.securityfocus.com/bid/20138>

* FRSIRT: ADV-2007-3155

<http://www.frsirt.com/english/advisories/2007/3155>

* SECTrack: 1018687

<http://www.securitytracker.com/id?1018687>

* SECUNIA: 22048

<http://secunia.com/advisories/22048>

* SECUNIA: 27414

<http://secunia.com/advisories/27414>

* SREASON: 1631

<http://securityreason.com/securityalert/1631>

CVE Reference:

CVE-2006-4965 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2008-2752** Microsoft CVSS 2.0 Score = 7.1

Microsoft Word 2000 9.0.2812 and 2003 11.8106.8172 does not properly handle unordered lists, which allows user-assisted remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a crafted .doc file. NOTE: some of these details are obtained from third party information.

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

References:

<http://www.securityfocus.com/data/vulnerabilities/exploits/crash-word-1.doc>

<http://www.securityfocus.com/data/vulnerabilities/exploits/crash-word-2.doc>

<http://www.securityfocus.com/data/vulnerabilities/exploits/crash-word-3.doc>

<http://www.securityfocus.com/data/vulnerabilities/exploits/crash-word-4.doc>

BID: <http://www.securityfocus.com/bid/29769>

CVE Reference: [CVE-2008-2752](#)

- **CVE-2008-2841** Microsoft CVSS 2.0 Score = 6.8

Argument injection vulnerability in XChat 2.8.7b and earlier on Windows, when Internet Explorer is used, allows remote attackers to execute arbitrary commands via the --command parameter in an ircs:// URI.

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

References:

MILWORM: <http://www.milw0rm.com/exploits/5795>

<http://forum.xchat.org/viewtopic.php?t=4218>

SECUNIA: <http://secunia.com/advisories/30695>

CVE Reference: [CVE-2008-2841](#)

- **CVE-2008-2794** Symantec CVSS 2.0 Score = 6.8

Unspecified vulnerability in the GUI in Symantec Altiris Notification Server Agent 6.x before 6.0 SP3 R8 allows local users to gain privileges via unknown attack vectors.

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

References:

<http://securityresponse.symantec.com/avcenter/security/Content/2008.06.17.html>

BID: <http://www.securityfocus.com/bid/29708>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/1861/references>

SECTRACK: <http://www.securitytracker.com/id?1020304>

SECUNIA: <http://secunia.com/advisories/30741>

CVE Reference: [CVE-2008-2794](#)

• **CVE-2008-2060 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability in Cisco Intrusion Prevention System (IPS) 5.x before 5.1(8)E2 and 6.x before 6.0(5)E2, when inline mode and jumbo Ethernet support are enabled, allows remote attackers to cause a denial of service (panic), and possibly bypass intended restrictions on network traffic, via a "specific series of jumbo Ethernet frames."

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

References:

CISCO:

http://www.cisco.com/en/US/products/products_security_advisory09186a00809b3842.shtml

CVE Reference: [CVE-2008-2060](#)

• **CVE-2008-2786 Mozilla CVSS 2.0 Score = 10.0**

Buffer overflow in Firefox 3.0 and 2.0.x has unknown impact and attack vectors. NOTE: due to lack of details as of 20080619, it is not clear whether this is the same issue as CVE-2008-2785. A CVE identifier has been assigned for tracking purposes.

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

References:

FULLDISC: <http://lists.grok.org.uk/pipermail/full-disclosure/2008-June/062832.html>

BID: <http://www.securityfocus.com/bid/29794>

CVE Reference: [CVE-2008-2786](#)

- **CVE-2008-2306 Apple CVSS 2.0 Score = 9.3**

Apple Safari before 3.1.2 on Windows does not follow certain Internet Explorer zone settings that limit the automatic downloading of files and automatic launching of executables, which allows remote attackers to bypass intended access restrictions and execute arbitrary code.

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

References:

APPLE: <http://lists.apple.com/archives/security-announce/2008//Jun/msg00001.html>

CVE Reference: [CVE-2008-2306](#)

- **CVE-2008-2307 Apple CVSS 2.0 Score = 9.3**

Unspecified vulnerability in WebKit in Apple Safari before 3.1.2 on Windows allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via vectors involving JavaScript arrays that trigger memory corruption.

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

References:

APPLE: <http://lists.apple.com/archives/security-announce/2008//Jun/msg00001.html>

BID: <http://www.securityfocus.com/bid/29836>

CVE Reference: [CVE-2008-2307](#)

- **CVE-2008-2785 Mozilla CVSS 2.0 Score = 9.3**

Unspecified vulnerability in Firefox 3.0 and 2.0.x has unknown impact and remote attack vectors, aka ZDI-CAN-349.

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

References:

<http://dvlabs.tippingpoint.com/blog/2008/06/18/vulnerability-in-mozilla-firefox-30>

BID: <http://www.securityfocus.com/bid/29802>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/1873>

SECUNIA: <http://secunia.com/advisories/30761>

XF: <http://xforce.iss.net/xforce/xfdb/43167>

CVE Reference: [CVE-2008-2785](https://cve.mitre.org/cve/2008/2785)

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