

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

A call for a new security model. Michael Barret on current security events. Security holes that could enable hackers to shop for free found. US officials turning off malware on infected PCs.

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

• Security fragmentation needs to end

Network World - A new week, a new rash of attacks against security vendors, email marketers and banks. It would be easy to point fingers and laugh at the irony, especially in the case of security vendors, but that would be both petty and shortsighted.

More on network security problems: 10 of the Worst Moments in Network Security History

The stark reality is that security breaches can, will and do happen to everyone. For every security control and process we put in place, somewhere else there's a vulnerability, a weakness, an untrained employee or a path of least resistance for an attack. All the point solutions in the world are not going to make us any more secure. What we desperately need is a new model for integrating security solutions across vendors, across devices, across operating systems and across the globe. Computerworld

Full Story :

http://www.computerworld.com/s/article/9215802/Security_fragmentation_needs_to_end?source=rss_security&utm

• PayPal security chief on Epsilon breach and more (Q&A)

Michael Barrett, chief information security officer at PayPal

(Credit: PayPal)

CNET got a few minutes on the phone today with Michael Barrett, chief information security officer at online payment processor PayPal, and asked him his opinion on some current events in the world of security. Here are edited excerpts of the interview with the man responsible for making sure the personal and financial data of millions of PayPal customers and thousands of employees is secure. *Cnet Security*

Full Story :

http://news.cnet.com/8301-27080_3-20052310-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• Could criminals shop for free online?

A group of security researchers say they have found ways to trick online cashier systems into ordering items for free or at a discount.

Researchers from Indiana University and Microsoft Research found security holes in a software development kit from payment hosting provider Amazon Payments, Rui Wang, a Ph.D. student at Indiana University, told CNET in a recent interview. Amazon fixed the problems after being notified by the researchers, and integration bugs found in merchant shopping-cart applications and implementations on several retail sites have also been fixed. *Cnet Security*

Full Story :

http://news.cnet.com/8301-27080_3-20049044-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• U.S. shuts botnet, can disable malware remotely

By seizing servers and domain names and getting permission to remotely turn off malware on compromised PCs, U.S. officials have disabled a botnet that steals data from infected computers.

The legal actions are part of the "most complete and comprehensive enforcement action ever taken by U.S. authorities to disable an international botnet," according to a statement from the Department of Justice. A botnet is a group of computers that have been compromised and are being remotely controlled by attackers, typically to send spam or attack other computers.

It's the first time law enforcement in the U.S. has requested permission from a court to take control of a botnet, according to a request for a temporary restraining order that was granted. Similar action was taken by Dutch officials who downloaded "good" software to computers infected with Bredolab botnet malware, the filing said. *Cnet Security*

Full Story :

http://news.cnet.com/8301-27080_3-20053708-245.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 19164 SSL renegotiation supported

The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.

This test case tests if the target's SSL layer accepts SSL renegotiation requests from clients.

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

References:

* BUGTRAQ: 20091124 rPSA-2009-0155-1 httpd mod_ssl

<http://www.securityfocus.com/archive/1/archive/1/508075/100/0/threaded>

* BUGTRAQ: 20091118 TLS / SSLv3 vulnerability explained (DRAFT)

<http://www.securityfocus.com/archive/1/archive/1/507952/100/0/threaded>

* BUGTRAQ: 20091130 TLS / SSLv3 vulnerability explained (New ways to leverage the vulnerability)

<http://www.securityfocus.com/archive/1/archive/1/508130/100/0/threaded>

* BUGTRAQ: 20101207 VMSA-2010-0019 VMware ESX third party updates for Service Console

<http://www.securityfocus.com/archive/1/archive/1/515055/100/0/threaded>

* BUGTRAQ: 20110211 VMSA-2011-0003 Third party component updates for VMware vCenter Server, vCenter Update Manager, ESXi and ESX
<http://www.securityfocus.com/archive/1/archive/1/516397/100/0/threaded>

* FULLDISC: 20091111 Re: SSL/TLS MiTM PoC
<http://seclists.org/fulldisclosure/2009/Nov/139>

* MLIST: [announce] 20091107 CVE-2009-3555 - apache/mod_ssl vulnerability and mitigation
<http://marc.info/?l=apache-httpd-announce&m=125755783724966&w=2>

* MLIST: [cryptography] 20091105 OpenSSL 0.9.8l released
<http://marc.info/?l=cryptography&m=125752275331877&w=2>

* MLIST: [gnutls-devel] 20091105 Re: TLS renegotiation MITM
<http://lists.gnu.org/archive/html/gnutls-devel/2009-11/msg00029.html>

* MLIST: [oss-security] 20091105 CVE-2009-3555 for TLS renegotiation MITM attacks
<http://www.openwall.com/lists/oss-security/2009/11/05/3>

* MLIST: [oss-security] 20091105 Re: CVE-2009-3555 for TLS renegotiation MITM attacks
<http://www.openwall.com/lists/oss-security/2009/11/05/5>

* MLIST: [oss-security] 20091107 Re: CVE-2009-3555 for TLS renegotiation MITM attacks
<http://www.openwall.com/lists/oss-security/2009/11/06/3>

* MLIST: [oss-security] 20091107 Re: [TLS] CVE-2009-3555 for TLS renegotiation MITM attacks
<http://www.openwall.com/lists/oss-security/2009/11/07/3>

* MLIST: [tls] 20091104 MITM attack on delayed TLS-client auth through renegotiation
<http://www.ietf.org/mail-archive/web/tls/current/msg03928.html>

* MLIST: [tls] 20091104 TLS renegotiation issue
<http://www.ietf.org/mail-archive/web/tls/current/msg03948.html>

* MLIST: [oss-security] 20091120 CVEs for nginx
<http://www.openwall.com/lists/oss-security/2009/11/20/1>

* MLIST: [oss-security] 20091123 Re: CVEs for nginx
<http://www.openwall.com/lists/oss-security/2009/11/23/10>

* MISC:
<http://extendedsubset.com/?p=8>

* MISC:
http://extendedsubset.com/Renegotiating_TLS.pdf

* MISC:
<http://www.betanews.com/article/1257452450>

* MISC:
http://www.educatedguesswork.org/2009/11/understanding_the_tls_renegoti.html

* MISC:
<http://www.tombom.co.uk/blog/?p=85>

* MISC:
https://bugzilla.mozilla.org/show_bug.cgi?id=526689

* MISC:
<https://svn.resiprocate.org/rep/ietf-drafts/ekr/draft-rescorla-tls-renegotiate.txt>

* MISC:
<http://blogs.iss.net/archive/sslmitmiscrf.html>

* MISC:
<http://www.securegoose.org/2009/11/tls-renegotiation-vulnerability-cve.html>

* MISC:
<http://blog.g-sec.lu/2009/11/tls-sslv3-renegotiation-vulnerability.html>

* MISC:
<http://clicky.me/tlsvuln>

* MISC:
<https://support.f5.com/kb/en-us/solutions/public/10000/700/sol10737.html>

* CONFIRM:
http://blogs.sun.com/security/entry/vulnerability_in_tls_protocol_during

* CONFIRM:
<http://kbase.redhat.com/faq/docs/DOC-20491>

* CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=533125

* CONFIRM:
<http://support.citrix.com/article/CTX123359>

* CONFIRM:
<http://sysoev.ru/nginx/patch.cve-2009-3555.txt>

* CONFIRM:
<http://wiki.rpath.com/Advisories:rPSA-2009-0155>

* CONFIRM:
<http://www.ingate.com/Relnote.php?ver=481>

* CONFIRM:
<http://www-01.ibm.com/support/docview.wss?uid=swg24025312>

* CONFIRM:
http://www.proftpd.org/docs/RELEASE_NOTES-1.3.2c

* CONFIRM:
<http://support.apple.com/kb/HT4004>

* CONFIRM:
http://support.zeus.com/zws/media/docs/4.3/RELEASE_NOTES

* CONFIRM:
http://support.zeus.com/zws/news/2010/01/13/zws_4_3r5_released

* CONFIRM:
<http://support.avaya.com/css/P8/documents/100070150>

* CONFIRM:
<http://www.mozilla.org/security/announce/2010/mfsa2010-22.html>

* CONFIRM:
https://bugzilla.mozilla.org/show_bug.cgi?id=545755

* CONFIRM:
<http://www-01.ibm.com/support/docview.wss?uid=swg21426108>

* CONFIRM:
<http://support.avaya.com/css/P8/documents/100081611>

* CONFIRM:
<http://support.apple.com/kb/HT4170>

* CONFIRM:
<http://support.apple.com/kb/HT4171>

* CONFIRM:
<http://www.openoffice.org/security/cves/CVE-2009-3555.html>

* CONFIRM:
<http://www.opera.com/docs/changelogs/unix/1060/>

* CONFIRM:
<http://www.opera.com/support/search/view/944/>

* CONFIRM:
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuijul2010.html>

* CONFIRM:
<http://www-01.ibm.com/support/docview.wss?uid=swg21432298>

* CONFIRM:
<http://support.avaya.com/css/P8/documents/100114315>

* CONFIRM:
<http://support.avaya.com/css/P8/documents/100114327>

* CONFIRM:
<http://www.oracle.com/technetwork/topics/security/javacpuoct2010-176258.html>

* CONFIRM:
<http://www.hitachi.co.jp/Prod/comp/soft1/security/info/vuls/HS10-030/index.html>

* CONFIRM:
<http://www-01.ibm.com/support/docview.wss?uid=swg24006386>

* CONFIRM:
<http://www.vmware.com/security/advisories/VMSA-2010-0019.html>

* CONFIRM:
<https://kb.bluecoat.com/index?page=content&id=SA50>

* CONFIRM:
<http://www.vmware.com/security/advisories/VMSA-2011-0003.html>

* CONFIRM:
http://www.vmware.com/support/vsphere4/doc/vsp_vc41_u1_rel_notes.html

* AIXAPAR: PM00675
<http://www-1.ibm.com/support/search.wss?rs=0&q=PM00675&apar=only>

* AIXAPAR: IC67848
<http://www-01.ibm.com/support/docview.wss?uid=swg1IC67848>

* AIXAPAR: PM12247
<http://www-01.ibm.com/support/docview.wss?uid=swg1PM12247>

* AIXAPAR: IC68054
<http://www-01.ibm.com/support/docview.wss?uid=swg1IC68054>

* AIXAPAR: IC68055
<http://www-01.ibm.com/support/docview.wss?uid=swg1IC68055>

* APPLE: APPLE-SA-2010-01-19-1
<http://lists.apple.com/archives/security-announce/2010/Jan/msg00000.html>

* APPLE: APPLE-SA-2010-05-18-1
<http://lists.apple.com/archives/security-announce/2010/May/msg00001.html>

* APPLE: APPLE-SA-2010-05-18-2
<http://lists.apple.com/archives/security-announce/2010/May/msg00002.html>

* CISCO: 20091109 Transport Layer Security Renegotiation Vulnerability
http://www.cisco.com/en/US/products/products_security_advisory09186a0080b01d1d.shtml

* DEBIAN: DSA-1934
<http://www.debian.org/security/2009/dsa-1934>

* DEBIAN: DSA-2141

<http://www.debian.org/security/2011/dsa-2141>

* FEDORA: FEDORA-2009-12750

<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00428.html>

* FEDORA: FEDORA-2009-12775

<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00442.html>

* FEDORA: FEDORA-2009-12782

<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00449.html>

* FEDORA: FEDORA-2009-12968

<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00634.html>

* FEDORA: FEDORA-2009-12604

<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00645.html>

* FEDORA: FEDORA-2009-12229

<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg01029.html>

* FEDORA: FEDORA-2009-12305

<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg01020.html>

* FEDORA: FEDORA-2009-12606

<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg00944.html>

* FEDORA: FEDORA-2010-5357

<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/039561.html>

* FEDORA: FEDORA-2010-5942

<http://lists.fedoraproject.org/pipermail/package-announce/2010-April/039957.html>

* FEDORA: FEDORA-2010-6131

<http://lists.fedoraproject.org/pipermail/package-announce/2010-May/040652.html>

* FEDORA: FEDORA-2010-16240

<http://lists.fedoraproject.org/pipermail/package-announce/2010-October/049702.html>

* FEDORA: FEDORA-2010-16294

<http://lists.fedoraproject.org/pipermail/package-announce/2010-October/049528.html>

* FEDORA: FEDORA-2010-16312

<http://lists.fedoraproject.org/pipermail/package-announce/2010-October/049455.html>

* GENTOO: GLSA-200912-01

<http://security.gentoo.org/glsa/glsa-200912-01.xml>

* HP: HPSBUX02482

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01945686>

* HP: HPSBMA02534

<http://marc.info/?l=bugtraq&w=2>

* HP: HPSBMA02547

http://itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02273751

* HP: HPSBGN02562

<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02436041>

* HP: HPSBMA02568

http://www.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c02512995

* MANDRIVA: MDVSA-2010:084

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:084>

* MANDRIVA: MDVSA-2010:076

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:076>

* MANDRIVA: MDVSA-2010:089

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:089>

* MS: MS10-049

<http://www.microsoft.com/technet/security/Bulletin/MS10-049.mspx>

* OPENBSD: [4.5] 010: SECURITY FIX: November 26, 2009

http://openbsd.org/errata45.html#010_openssl

* OPENBSD: [4.6] 004: SECURITY FIX: November 26, 2009

http://openbsd.org/errata46.html#004_openssl

* REDHAT: RHSA-2010:0119

<http://www.redhat.com/support/errata/RHSA-2010-0119.html>

* REDHAT: RHSA-2010:0155

<http://www.redhat.com/support/errata/RHSA-2010-0155.html>

* REDHAT: RHSA-2010:0167

<http://www.redhat.com/support/errata/RHSA-2010-0167.html>

* REDHAT: RHSA-2010:0337

<http://www.redhat.com/support/errata/RHSA-2010-0337.html>

* REDHAT: RHSA-2010:0338

<http://www.redhat.com/support/errata/RHSA-2010-0338.html>

* REDHAT: RHSA-2010:0339

<http://www.redhat.com/support/errata/RHSA-2010-0339.html>

* REDHAT: RHSA-2010:0130

<http://www.redhat.com/support/errata/RHSA-2010-0130.html>

* REDHAT: RHSA-2010:0165

<http://www.redhat.com/support/errata/RHSA-2010-0165.html>

* REDHAT: RHSA-2010:0770
<http://www.redhat.com/support/errata/RHSA-2010-0770.html>

* REDHAT: RHSA-2010:0786
<http://www.redhat.com/support/errata/RHSA-2010-0786.html>

* REDHAT: RHSA-2010:0807
<http://www.redhat.com/support/errata/RHSA-2010-0807.html>

* REDHAT: RHSA-2010:0768
<http://www.redhat.com/support/errata/RHSA-2010-0768.html>

* REDHAT: RHSA-2010:0865
<http://www.redhat.com/support/errata/RHSA-2010-0865.html>

* REDHAT: RHSA-2010:0986
<http://www.redhat.com/support/errata/RHSA-2010-0986.html>

* REDHAT: RHSA-2010:0987
<http://www.redhat.com/support/errata/RHSA-2010-0987.html>

* SLACKWARE: SSA:2009-320-01
<http://slackware.com/security/viewer.php?l=slackware-security&v=2009&m=slackware-security.597446>

* SUNALERT: 273029
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-273029-1>

* SUNALERT: 273350
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-273350-1>

* SUNALERT: 274990
<http://sunsolve.sun.com/search/document.do?assetkey=1-66-274990-1>

* SUNALERT: 1021752
<http://sunsolve.sun.com/search/document.do?assetkey=1-77-1021752.1-1>

* SUNALERT: 1021653
<http://sunsolve.sun.com/search/document.do?assetkey=1-77-1021653.1-1>

* SUSE: SUSE-SA:2009:057
<http://lists.opensuse.org/opensuse-security-announce/2009-11/msg00009.html>

* SUSE: SUSE-SR:2010:008
<http://lists.opensuse.org/opensuse-security-announce/2010-04/msg00001.html>

* SUSE: SUSE-SR:2010:011
<http://lists.opensuse.org/opensuse-security-announce/2010-05/msg00001.html>

* SUSE: SUSE-SR:2010:012
<http://lists.opensuse.org/opensuse-security-announce/2010-05/msg00002.html>

* SUSE: SUSE-SR:2010:013
<http://lists.opensuse.org/opensuse-security-announce/2010-06/msg00001.html>

* SUSE: SUSE-SA:2010:061
<http://lists.opensuse.org/opensuse-security-announce/2010-12/msg00005.html>

* SUSE: SUSE-SR:2010:019
<http://lists.opensuse.org/opensuse-security-announce/2010-10/msg00006.html>

* SUSE: SUSE-SR:2010:024
<http://lists.opensuse.org/opensuse-security-announce/2010-12/msg00006.html>

* UBUNTU: USN-923-1
<http://ubuntu.com/usn/usn-923-1>

* UBUNTU: USN-927-1
<http://www.ubuntu.com/usn/USN-927-1>

* UBUNTU: USN-927-4
<http://www.ubuntu.com/usn/USN-927-4>

* UBUNTU: USN-927-5
<http://www.ubuntu.com/usn/USN-927-5>

* UBUNTU: USN-1010-1
<http://www.ubuntu.com/usn/USN-1010-1>

* CERT: TA10-222A
<http://www.us-cert.gov/cas/techalerts/TA10-222A.html>

* CERT: TA10-287A
<http://www.us-cert.gov/cas/techalerts/TA10-287A.html>

* CERT-VN: VU#120541
<http://www.kb.cert.org/vuls/id/120541>

* BID: 36935
<http://www.securityfocus.com/bid/36935>

* OSVDB: 60521
<http://osvdb.org/60521>

* OSVDB: 60972
<http://osvdb.org/60972>

* OSVDB: 62210
<http://osvdb.org/62210>

* OSVDB: 65202
<http://osvdb.org/65202>

* OVAL: oval:org.mitre.oval:def:10088

<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:10088>
* OVAL: oval:org.mitre.oval:def:11578
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:11578>
* OVAL: oval:org.mitre.oval:def:7315
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7315>
* OVAL: oval:org.mitre.oval:def:7973
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:7973>
* OVAL: oval:org.mitre.oval:def:8366
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8366>
* OVAL: oval:org.mitre.oval:def:8535
<http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:8535>
* SECTRACK: 1023148
<http://securitytracker.com/id?1023148>
* SECTRACK: 1023163
<http://www.securitytracker.com/id?1023163>
* SECTRACK: 1023204
<http://www.securitytracker.com/id?1023204>
* SECTRACK: 1023205
<http://www.securitytracker.com/id?1023205>
* SECTRACK: 1023206
<http://www.securitytracker.com/id?1023206>
* SECTRACK: 1023207
<http://www.securitytracker.com/id?1023207>
* SECTRACK: 1023208
<http://www.securitytracker.com/id?1023208>
* SECTRACK: 1023209
<http://www.securitytracker.com/id?1023209>
* SECTRACK: 1023210
<http://www.securitytracker.com/id?1023210>
* SECTRACK: 1023211
<http://www.securitytracker.com/id?1023211>
* SECTRACK: 1023212
<http://www.securitytracker.com/id?1023212>
* SECTRACK: 1023215
<http://www.securitytracker.com/id?1023215>
* SECTRACK: 1023216
<http://www.securitytracker.com/id?1023216>
* SECTRACK: 1023217
<http://www.securitytracker.com/id?1023217>
* SECTRACK: 1023218
<http://www.securitytracker.com/id?1023218>
* SECTRACK: 1023219
<http://www.securitytracker.com/id?1023219>
* SECTRACK: 1023243
<http://www.securitytracker.com/id?1023243>
* SECTRACK: 1023270
<http://www.securitytracker.com/id?1023270>
* SECTRACK: 1023271
<http://www.securitytracker.com/id?1023271>
* SECTRACK: 1023272
<http://www.securitytracker.com/id?1023272>
* SECTRACK: 1023273
<http://www.securitytracker.com/id?1023273>
* SECTRACK: 1023274
<http://www.securitytracker.com/id?1023274>
* SECTRACK: 1023275
<http://www.securitytracker.com/id?1023275>
* SECTRACK: 1023411
<http://www.securitytracker.com/id?1023411>
* SECTRACK: 1023426
<http://www.securitytracker.com/id?1023426>
* SECTRACK: 1023427
<http://www.securitytracker.com/id?1023427>
* SECTRACK: 1023428
<http://www.securitytracker.com/id?1023428>
* SECTRACK: 1023213
<http://www.securitytracker.com/id?1023213>
* SECTRACK: 1023214
<http://www.securitytracker.com/id?1023214>

* SECTRACK: 1023224
<http://www.securitytracker.com/id?1023224>
* SECTRACK: 1024789
<http://www.securitytracker.com/id?1024789>
* SECUNIA: 37291
<http://secunia.com/advisories/37291>
* SECUNIA: 37292
<http://secunia.com/advisories/37292>
* SECUNIA: 37320
<http://secunia.com/advisories/37320>
* SECUNIA: 37501
<http://secunia.com/advisories/37501>
* SECUNIA: 37504
<http://secunia.com/advisories/37504>
* SECUNIA: 37656
<http://secunia.com/advisories/37656>
* SECUNIA: 37675
<http://secunia.com/advisories/37675>
* SECUNIA: 37604
<http://secunia.com/advisories/37604>
* SECUNIA: 37640
<http://secunia.com/advisories/37640>
* SECUNIA: 37859
<http://secunia.com/advisories/37859>
* SECUNIA: 38056
<http://secunia.com/advisories/38056>
* SECUNIA: 38241
<http://secunia.com/advisories/38241>
* SECUNIA: 38484
<http://secunia.com/advisories/38484>
* SECUNIA: 38003
<http://secunia.com/advisories/38003>
* SECUNIA: 38020
<http://secunia.com/advisories/38020>
* SECUNIA: 38687
<http://secunia.com/advisories/38687>
* SECUNIA: 39136
<http://secunia.com/advisories/39136>
* SECUNIA: 39242
<http://secunia.com/advisories/39242>
* SECUNIA: 39243
<http://secunia.com/advisories/39243>
* SECUNIA: 39292
<http://secunia.com/advisories/39292>
* SECUNIA: 39317
<http://secunia.com/advisories/39317>
* SECUNIA: 37383
<http://secunia.com/advisories/37383>
* SECUNIA: 37399
<http://secunia.com/advisories/37399>
* SECUNIA: 37453
<http://secunia.com/advisories/37453>
* SECUNIA: 39278
<http://secunia.com/advisories/39278>
* SECUNIA: 38781
<http://secunia.com/advisories/38781>
* SECUNIA: 39500
<http://secunia.com/advisories/39500>
* SECUNIA: 39628
<http://secunia.com/advisories/39628>
* SECUNIA: 39461
<http://secunia.com/advisories/39461>
* SECUNIA: 39632
<http://secunia.com/advisories/39632>
* SECUNIA: 39713
<http://secunia.com/advisories/39713>
* SECUNIA: 39819
<http://secunia.com/advisories/39819>
* SECUNIA: 40070

<http://secunia.com/advisories/40070>
* SECUNIA: 39127
<http://secunia.com/advisories/39127>
* SECUNIA: 40545
<http://secunia.com/advisories/40545>
* SECUNIA: 40747
<http://secunia.com/advisories/40747>
* SECUNIA: 40866
<http://secunia.com/advisories/40866>
* SECUNIA: 41480
<http://secunia.com/advisories/41480>
* SECUNIA: 41490
<http://secunia.com/advisories/41490>
* SECUNIA: 41967
<http://secunia.com/advisories/41967>
* SECUNIA: 41972
<http://secunia.com/advisories/41972>
* SECUNIA: 42377
<http://secunia.com/advisories/42377>
* SECUNIA: 42379
<http://secunia.com/advisories/42379>
* SECUNIA: 42467
<http://secunia.com/advisories/42467>
* SECUNIA: 42811
<http://secunia.com/advisories/42811>
* SECUNIA: 42724
<http://secunia.com/advisories/42724>
* SECUNIA: 42733
<http://secunia.com/advisories/42733>
* SECUNIA: 42808
<http://secunia.com/advisories/42808>
* SECUNIA: 42816
<http://secunia.com/advisories/42816>
* SECUNIA: 43308
<http://secunia.com/advisories/43308>
* VUPEN: ADV-2009-3164
<http://www.vupen.com/english/advisories/2009/3164>
* VUPEN: ADV-2009-3165
<http://www.vupen.com/english/advisories/2009/3165>
* VUPEN: ADV-2009-3205
<http://www.vupen.com/english/advisories/2009/3205>
* VUPEN: ADV-2009-3220
<http://www.vupen.com/english/advisories/2009/3220>
* VUPEN: ADV-2009-3353
<http://www.vupen.com/english/advisories/2009/3353>
* VUPEN: ADV-2009-3354
<http://www.vupen.com/english/advisories/2009/3354>
* VUPEN: ADV-2009-3484
<http://www.vupen.com/english/advisories/2009/3484>
* VUPEN: ADV-2009-3521
<http://www.vupen.com/english/advisories/2009/3521>
* VUPEN: ADV-2009-3587
<http://www.vupen.com/english/advisories/2009/3587>
* VUPEN: ADV-2010-0173
<http://www.vupen.com/english/advisories/2010/0173>
* VUPEN: ADV-2010-0086
<http://www.vupen.com/english/advisories/2010/0086>
* VUPEN: ADV-2010-0748
<http://www.vupen.com/english/advisories/2010/0748>
* VUPEN: ADV-2009-3310
<http://www.vupen.com/english/advisories/2009/3310>
* VUPEN: ADV-2009-3313
<http://www.vupen.com/english/advisories/2009/3313>
* VUPEN: ADV-2010-0848
<http://www.vupen.com/english/advisories/2010/0848>
* VUPEN: ADV-2010-0982
<http://www.vupen.com/english/advisories/2010/0982>
* VUPEN: ADV-2010-0933
<http://www.vupen.com/english/advisories/2010/0933>

* VUPEN: ADV-2010-0916
<http://www.vupen.com/english/advisories/2010/0916>
* VUPEN: ADV-2010-1054
<http://www.vupen.com/english/advisories/2010/1054>
* VUPEN: ADV-2010-0994
<http://www.vupen.com/english/advisories/2010/0994>
* VUPEN: ADV-2010-1107
<http://www.vupen.com/english/advisories/2010/1107>
* VUPEN: ADV-2010-1191
<http://www.vupen.com/english/advisories/2010/1191>
* VUPEN: ADV-2010-1350
<http://www.vupen.com/english/advisories/2010/1350>
* VUPEN: ADV-2010-1673
<http://www.vupen.com/english/advisories/2010/1673>
* VUPEN: ADV-2010-1639
<http://www.vupen.com/english/advisories/2010/1639>
* VUPEN: ADV-2010-1793
<http://www.vupen.com/english/advisories/2010/1793>
* VUPEN: ADV-2010-2010
<http://www.vupen.com/english/advisories/2010/2010>
* VUPEN: ADV-2010-2745
<http://www.vupen.com/english/advisories/2010/2745>
* VUPEN: ADV-2010-3069
<http://www.vupen.com/english/advisories/2010/3069>
* VUPEN: ADV-2010-3086
<http://www.vupen.com/english/advisories/2010/3086>
* VUPEN: ADV-2010-3126
<http://www.vupen.com/english/advisories/2010/3126>
* VUPEN: ADV-2011-0032
<http://www.vupen.com/english/advisories/2011/0032>
* VUPEN: ADV-2011-0033
<http://www.vupen.com/english/advisories/2011/0033>
* VUPEN: ADV-2011-0086
<http://www.vupen.com/english/advisories/2011/0086>
* XF: tls-renegotiation-weak-security(54158)
<http://xforce.iss.net/xforce/xfdb/54158>

CVE Reference:

CVE-2009-3555 (cve.mitre.org, nvd.nist.gov)

• 19255 Layouts Handling Memory Corruption Vulnerability (MS11-018/2497640) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. 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.

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

References:

* MS: MS11-018
<http://www.microsoft.com/technet/security/Bulletin/MS11-018.mspx>
* BID: 47190
<http://www.securityfocus.com/bid/47190>
* VUPEN: VUPEN/ADV-2011-0937
<http://www.vupen.com/english/advisories/2011/0937>
* SECTRACK: 1025327
<http://www.securitytracker.com/id/1025327>

CVE Reference:

CVE-2011-0094 (cve.mitre.org, nvd.nist.gov)

• 19256 MSHTML Memory Corruption Vulnerability (MS11-018/2497640) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted

Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. 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.

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

References:

- * MS: MS11-018
<http://www.microsoft.com/technet/security/Bulletin/MS11-018.msp>
- * BID: 45639
<http://www.securityfocus.com/bid/45639>
- * VUPEN: VUPEN/ADV-2011-0937
<http://www.vupen.com/english/advisories/2011/0937>
- * SECTRACK: 1025327
<http://www.securitytracker.com/id/1025327>

CVE Reference:

CVE-2011-0346 (cve.mitre.org, nvd.nist.gov)

• 19257 Frame Tag Information Disclosure Vulnerability (MS11-018/2497640) (Remote File Checking)

An information disclosure vulnerability exists in Internet Explorer. An attacker could exploit the vulnerability by constructing a specially crafted Web page disguised as legitimate content. The user's actions on the page could allow information disclosure or clickjacking, whereby the user's clicks perform unwanted actions.

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

References:

- * MS: MS11-018
<http://www.microsoft.com/technet/security/Bulletin/MS11-018.msp>
- * BID: 47191
<http://www.securityfocus.com/bid/47191>
- * VUPEN: VUPEN/ADV-2011-0937
<http://www.vupen.com/english/advisories/2011/0937>
- * SECTRACK: 1025327
<http://www.securitytracker.com/id/1025327>

CVE Reference:

CVE-2011-1244 (cve.mitre.org, nvd.nist.gov)

• 19258 Javascript Information Disclosure Vulnerability (MS11-018/2497640) (Remote File Checking)

An information disclosure vulnerability exists in Internet Explorer that could allow script to gain access to information in another domain or Internet Explorer zone. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could allow information disclosure if a user viewed the Web page. An attacker who successfully exploited this vulnerability could view content from another domain or Internet Explorer zone.

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

References:

- * MS: MS11-018
<http://www.microsoft.com/technet/security/Bulletin/MS11-018.msp>
- * BID: 47192
<http://www.securityfocus.com/bid/47192>
- * VUPEN: VUPEN/ADV-2011-0937
<http://www.vupen.com/english/advisories/2011/0937>
- * SECTRACK: 1025327
<http://www.securitytracker.com/id/1025327>

CVE Reference:

CVE-2011-1245 (cve.mitre.org, nvd.nist.gov)

• 19259 Object Management Memory Corruption Vulnerability (MS11-018/2497640) (Remote File Checking)

A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted

Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. 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.

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

References:

- * MS: MS11-018
<http://www.microsoft.com/technet/security/Bulletin/MS11-018.mspx>
- * BID: 46821
<http://www.securityfocus.com/bid/46821>
- * VUPEN: VUPEN/ADV-2011-0937
<http://www.vupen.com/english/advisories/2011/0937>
- * SECTRACK: 1025327
<http://www.securitytracker.com/id/1025327>

CVE Reference:

CVE-2011-1345 (cve.mitre.org, nvd.nist.gov)

• 19260 Browser Pool Corruption Vulnerability (MS11-019/2511455) (Remote File Checking)

An unauthenticated remote code execution vulnerability exists in the way that the Common Internet File System (CIFS) Browser Protocol implementation parses malformed browser messages. An attempt to exploit the vulnerability would not require authentication. An attacker who successfully exploited this vulnerability could execute arbitrary code and take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

- * MS: MS11-019
<http://www.microsoft.com/technet/security/Bulletin/MS11-019.mspx>
- * EXPLOIT-DB: 16166
<http://www.exploit-db.com/exploits/16166>
- * FULLDISC: 20110214 MS Windows Server 2003 AD Pre-Auth BROWSER ELECTION Remote Heap Overflow
<http://archives.neohapsis.com/archives/fulldisclosure/current/0284.html>
- * CONFIRM:
<http://blogs.technet.com/b/mmpc/archive/2011/02/16/my-sweet-valentine-the-cifs-browser-protocol-heap-corruption-vulnerability.aspx>
- * CONFIRM:
<http://blogs.technet.com/b/srd/archive/2011/02/16/notes-on-exploitability-of-the-recent-windows-browser-protocol-issue.aspx>
- * BID: 46360
<http://www.securityfocus.com/bid/46360>
- * SECUNIA: 43299
<http://secunia.com/advisories/43299>
- * VUPEN: ADV-2011-0394
<http://www.vupen.com/english/advisories/2011/0394>
- * XF: ms-win-server-browser-bo(65376)
<http://xforce.iss.net/xforce/xfdb/65376>
- * SECTRACK: 1025328
<http://www.securitytracker.com/id/1025328>

CVE Reference:

CVE-2011-0654 (cve.mitre.org, nvd.nist.gov)

• 19261 SMB Client Response Parsing Vulnerability (MS11-019/2511455) (Remote File Checking)

An unauthenticated remote code execution vulnerability exists in the way that the Microsoft Server Message Block (SMB) client validates specially crafted SMB responses. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB response to a client-initiated SMB request. An attacker who successfully exploited this vulnerability could execute arbitrary code and take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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

References:

* MS: MS11-019
<http://www.microsoft.com/technet/security/Bulletin/MS11-019.msp>
* SECTRACK: 1025328
<http://www.securitytracker.com/id/1025328>
* BID: 47239
<http://www.securityfocus.com/bid/47239>
* VUPEN: VUPEN/ADV-2011-0938
<http://www.vupen.com/english/advisories/2011/0938>

CVE Reference:

CVE-2011-0660 (cve.mitre.org, nvd.nist.gov)

• **19262 SMB Transaction Parsing Vulnerability (MS11-020/2508429) (Remote File Checking)**

An unauthenticated remote code execution vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted SMB packet to a computer running the Server service. An attacker who successfully exploited this vulnerability could take complete control of the system.

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

References:

* MS: MS11-020
<http://www.microsoft.com/technet/security/Bulletin/MS11-020.msp>
* SECTRACK: 1025329
<http://www.securitytracker.com/id/1025329>
* BID: 47198
<http://www.securityfocus.com/bid/47198>
* VUPEN: VUPEN/ADV-2011-0939
<http://www.vupen.com/english/advisories/2011/0939>

CVE Reference:

CVE-2011-0661 (cve.mitre.org, nvd.nist.gov)

• **19263 DNS Query Vulnerability (MS11-030/2509553) (Remote File Checking)**

A remote code execution vulnerability exists in the way that the DNS client service handles specially crafted LLMNR queries. An attacker who successfully exploited this vulnerability could run arbitrary code in the context of the NetworkService account. 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: MS11-030
<http://www.microsoft.com/technet/security/Bulletin/MS11-030.msp>
* SECTRACK: 1025332
<http://www.securitytracker.com/id/1025332>
* BID: 47242
<http://www.securityfocus.com/bid/47242>
* VUPEN: VUPEN/ADV-2011-0948
<http://www.vupen.com/english/advisories/2011/0948>

CVE Reference:

CVE-2011-0657 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2011-0661 Microsoft CVSS 2.0 Score = 10.0**

The SMB Server service in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate fields in SMB requests, which allows remote attackers to execute arbitrary code via a malformed request in a (1) SMBv1 or (2) SMBv2 packet, aka "SMB Transaction Parsing Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-020.msp>

CVE Reference: [CVE-2011-0661](#)

• **CVE-2011-0657 Microsoft CVSS 2.0 Score = 10.0**

DNSAPI.dll in the DNS client in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process DNS queries, which allows remote attackers to execute arbitrary code via (1) a crafted LLMNR broadcast query or (2) a crafted application, aka "DNS Query Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-030.msp>

CVE Reference: [CVE-2011-0657](#)

• **CVE-2011-0655 Microsoft CVSS 2.0 Score = 9.3**

Microsoft PowerPoint 2007 SP2 and 2010; Office 2004, 2008, and 2011 for Mac; Open XML File Format Converter for Mac; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP2; PowerPoint Viewer; PowerPoint Viewer 2007 SP2; and PowerPoint Web App do not properly validate TimeColorBehaviorContainer Floating Point records in PowerPoint documents, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted document containing an invalid record, aka "Floating Point Techno-color Time Bandit RCE Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-022.msp>

CVE Reference: [CVE-2011-0655](#)

• **CVE-2011-0663 Microsoft CVSS 2.0 Score = 9.3**

Multiple integer overflows in the Microsoft (1) JScript 5.6 through 5.8 and (2) VBScript 5.6 through 5.8 scripting engines allow remote attackers to execute arbitrary code via a crafted web page, aka "Scripting Memory Reallocation Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-031.msp>

CVE Reference: [CVE-2011-0663](#)

• **CVE-2011-0660 Microsoft CVSS 2.0 Score = 9.3**

The SMB client in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote SMB servers to execute arbitrary code via a crafted (1) SMBv1 or (2) SMBv2 response, aka "SMB Client Response Parsing Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-019.msp>

CVE Reference: [CVE-2011-0660](#)

• **CVE-2011-0656 Microsoft CVSS 2.0 Score = 9.3**

Microsoft PowerPoint 2002 SP3, 2003 SP3, 2007 SP2, and 2010; Office 2004, 2008, and 2011 for Mac; Open XML File Format Converter for Mac; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP2; PowerPoint Viewer; PowerPoint Viewer 2007 SP2; and PowerPoint Web App do not properly validate PersistDirectoryEntry records in PowerPoint documents, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted document containing an invalid record, aka "Persist Directory RCE Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-022.msp>

CVE Reference: [CVE-2011-0656](#)

• **CVE-2011-0107 Microsoft CVSS 2.0 Score = 9.3**

Untrusted search path vulnerability in Microsoft Office XP SP3, Office 2003 SP3, and Office 2007 SP2 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .docx file, aka "Office Component Insecure Library Loading Vulnerability." Per: <http://cwe.mitre.org/data/definitions/426.html> 'CWE-426: Untrusted Search Path'

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-023.msp>

CVE Reference: [CVE-2011-0107](#)

• **CVE-2011-0105 Microsoft CVSS 2.0 Score = 9.3**

Microsoft Excel 2002 SP3, Office 2004 and 2008 for Mac, and Open XML File Format Converter for Mac obtain a certain length value from an uninitialized memory location, which allows remote attackers to trigger a buffer overflow and execute arbitrary code via a crafted Excel file, aka "Excel Data Initialization Vulnerability."

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

References:

MS: <http://www.microsoft.com/technet/security/Bulletin/MS11-021.msp>

CVE Reference: [CVE-2011-0105](#)

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