netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 31

August 1, 2008

Table of Contents

Product Focus

Sasser Worm Scanner - The S4 Sasser Worm 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 SSL Vulnerability (MS04-011) that used by the Sasser Worm to infect machines.

This Week in Review

Senate approves harsher cyberattack restriction bill. Most banks are not secure. Applications getting weaker.

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

- **31 Jul 2008 15:42:45 Senate OKs revamped identity theft legislation**

An amended bill that would impose harsher restrictions on cyberattacks and allow identity theft victims to recoup costs in federal court passed the Senate on Wednesday.

The legislation, known as the Identity Theft Enforcement and Restitution Act,

isÂ included inÂ a U.S. House-approved bill that states that former vice presidents would receive U.S. Secret Service protection. The combined bill will now return to the House for consideration.

The bill, co-sponsored by Sens. Patrick Leahy, D-Vt., and Arlen Specter, R-Pa., had unanimously passed the Senate in November but had stalled in the House.

SC Magazine

Full story : **http://www.scmagazineus.com/Senate-OKs-revamped-identity-theft-legislation/article/113232/**

- **28 Jul 2008 17:47:26 Study: Security flaws threaten online banking**

More than 75 percent of bank websites have at least one design flaw that could lead to the theft of customer information, according to a recent University of Michigan study.

Sites forwarded users to new pages that had different domains without notifying the user from a secure page. There were login options on insecure pages. Contact information and security advice were shown on insecure pages. Policies for user IDs and passwords were inadequate. Design flaws such as these mean that customers may struggle to make the best security-related decision when entering confidential data, Laura Falk, who is pursuing a doctorate and is one of the researchers, told SCMagazineUS.com on Monday.

Gartner analyst Avivah Litan said that although most companies are good at protecting the login page, this study shows that security concerns appear to wane on other pages.

SC Magazine

Full story: **http://www.scmagazineus.com/Study-Security-flaws-threaten-online-banking/article/113010/**

- **28 Jul 2008 17:47:26 Study: Security flaws threaten online banking**

More than 75 percent of bank websites have at least one design flaw that could lead to the theft of customer information, according to a recent University of Michigan study.

Sites forwarded users to new pages that had different domains without notifying the user from a secure page. There were login options on insecure pages. Contact information and security advice were shown on insecure pages. Policies for user IDs and passwords were inadequate. Design flaws such as these mean that customers may struggle to make the best security-related decision when entering confidential data, Laura Falk, who is pursuing a doctorate and is one of the researchers, told

SCMagazineUS.com on Monday.

Gartner analyst Avivah Litan said that although most companies are good at protecting the login page, this study shows that security concerns appear to wane on other pages.

SC Magazine

Full story: **http://www.scmagazineus.com/Study-Security-flaws-threaten-online-banking/article/113010/**

- **25 Jul 2008 10:57:18 Application weaknesses double as networks tighten up**

An analysis of 100 security tests carried out over the past five years shows that application level weaknesses are up by 50 percent.

Security services provider Orthus conducted the baseline security tests beginning 2004 in terms of both network and application layers. The tests were carried out in industry sectors such as banking, insurance, finance, retail, manufacturing, transport, utilities, health and education.

The study revealed nearly 2,000 vulnerabilities. At least one security vulnerability was found at the network level in all tests and in 97 percent of the tests, at least one vulnerability was found at the application level.

Computerworld

Full story : **http://www.scmagazineus.com/Application-weaknesses-double-as-networks-tighten-up/article/112932/**

New Vulnerabilities Tested in SecureScout

- **16995 Oracle Application Server - Oracle HTTP Server component unspecified Vulnerability (jul-2008/CVE-2007-1359)**

An unspecified vulnerability with unknown impact exists in Oracle Application Server "Oracle HTTP Server" component.

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

References:

* MISC:
http://www.php-security.org/MOPB/BONUS-12-2007.html
* CONFIRM:
http://www.modsecurity.org/blog/archives/2007/03/modsecurity_asc.html

* CONFIRM:
http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujul2008.html
* GENTOO: GLSA-200705-17
http://www.gentoo.org/security/en/glsa/glsa-200705-17.xml
* BID: 22831
http://www.securityfocus.com/bid/22831
* FRSIRT: ADV-2007-0868
http://www.frsirt.com/english/advisories/2007/0868
* OSVDB: 32778
http://www.osvdb.org/32778
* SECUNIA: 24373
http://secunia.com/advisories/24373
* SECUNIA: 25316
http://secunia.com/advisories/25316
* XF: modsecurity-formurlencoded-security-bypass(32872)
http://xforce.iss.net/xforce/xfdb/32872

CVE Reference:

CVE-2007-1359 (cve.mitre.org, nvd.nist.gov)

- **18029 Apache, mod_proxy buffer overflow Vulnerability**

A buffer overflow was found in the Apache proxy module, mod_proxy, which can be triggered by receiving an invalid Content-Length header. In order to exploit this issue an attacker would need to get an Apache installation that was configured as a proxy to connect to a malicious site. This would cause the Apache child processing the request to crash, although this does not represent a significant Denial of Service attack as requests will continue to be handled by other Apache child processes. This issue may lead to remote arbitrary code execution on some BSD platforms.

The vulnerability has been confirmed in Apache 1.3.x up to 1.3.31.

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

References:

* FULLDISC: 20040610 Buffer overflow in apache mod_proxy,yet still apache much better than windows
http://seclists.org/lists/fulldisclosure/2004/Jun/0296.html
* MISC:
http://www.guninski.com/modproxy1.html
* BUGTRAQ: 20040611 [OpenPKG-SA-2004.029] OpenPKG Security Advisory (apache)
http://marc.theaimsgroup.com/?l=bugtraq&m=108711172710140&w=2
* DEBIAN: DSA-525
http://www.debian.org/security/2004/dsa-525
* MANDRAKE: MDKSA-2004:065
http://www.mandriva.com/security/advisories?name=MDKSA-2004:065
* REDHAT: RHSA-2004:245
http://rhn.redhat.com/errata/RHSA-2004-245.html
* SGI: 20040605-01-U

ftp://patches.sgi.com/support/free/security/advisories/20040605-01-U.asc
* SUNALERT: 57628
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57628-1
* SUNALERT: 101555
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101555-1
* SUNALERT: 101841
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101841-1
* CERT-VN: VU#541310
http://www.kb.cert.org/vuls/id/541310
* OVAL: oval:org.mitre.oval:def:4863
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4863
* OVAL: oval:org.mitre.oval:def:100112
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:100112
* SECUNIA: 11841
http://secunia.com/advisories/11841
* XF: apache-modproxy-contentlength-bo(16387)
http://xforce.iss.net/xforce/xfdb/16387

CVE Reference:

CVE-2004-0492 (cve.mitre.org, nvd.nist.gov)

- **18030 Apache, Expect header Cross-Site Scripting Vulnerability**

A flaw exists in the handling of invalid Expect headers. If an attacker can influence the Expect header that a victim sends to a target site they could perform a cross-site scripting attack. It is known that some versions of Flash can set an arbitrary Expect header which can trigger this flaw. Not marked as a security issue for 2.0 or 2.2 as the cross-site scripting is only returned to the victim after the server times out a connection.

The vulnerability has been confirmed in Apache 1.3.x up to 1.3.34.

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

References:

* BUGTRAQ: 20060508 Unfiltered Header Injection in Apache 1.3.34/2.0.57/2.2.1
http://archives.neohapsis.com/archives/bugtraq/2006-05/0151.html
* BUGTRAQ: 20060724 Write-up by Amit Klein:
http://archives.neohapsis.com/archives/bugtraq/2006-07/0425.html
* CONFIRM:
http://svn.apache.org/viewvc?view=rev&revision=394965
* CONFIRM:
http://support.avaya.com/elmodocs2/security/ASA-2006-194.htm
* CONFIRM:
http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd?mode=18&ID=3117
* CONFIRM:
http://kb.vmware.com/KanisaPlatform/Publishing/466/5915871_f.SAL_Public.html
* AIXAPAR: PK24631
http://www-1.ibm.com/support/docview.wss?uid=swg1PK24631
* AIXAPAR: PK27875

http://www-1.ibm.com/support/docview.wss?uid=swg24013080
* DEBIAN: DSA-1167
http://www.debian.org/security/2006/dsa-1167
* OPENBSD: [3.9] 012: SECURITY FIX: October 7, 2006
http://openbsd.org/errata.html#httpd2
* REDHAT: RHSA-2006:0618
http://rhn.redhat.com/errata/RHSA-2006-0618.html
* REDHAT: RHSA-2006:0619
http://www.redhat.com/support/errata/RHSA-2006-0619.html
* REDHAT: RHSA-2006:0692
http://rhn.redhat.com/errata/RHSA-2006-0692.html
* SGI: 20060801-01-P
ftp://patches.sgi.com/support/free/security/advisories/20060801-01-P
* SUSE: SUSE-SA:2006:051
http://www.novell.com/linux/security/advisories/2006_51_apache.html
* SUSE: SUSE-SA:2008:021
http://lists.opensuse.org/opensuse-security-announce/2008-04/msg00004.html
* UBUNTU: USN-575-1
http://www.ubuntu.com/usn/usn-575-1
* BID: 19661
http://www.securityfocus.com/bid/19661
* FRSIRT: ADV-2006-2963
http://www.frsirt.com/english/advisories/2006/2963
* FRSIRT: ADV-2006-2964
http://www.frsirt.com/english/advisories/2006/2964
* FRSIRT: ADV-2006-3264
http://www.frsirt.com/english/advisories/2006/3264
* FRSIRT: ADV-2006-4207
http://www.frsirt.com/english/advisories/2006/4207
* FRSIRT: ADV-2006-5089
http://www.frsirt.com/english/advisories/2006/5089
* SECTRACK: 1016569
http://securitytracker.com/id?1016569
* SECUNIA: 21172
http://secunia.com/advisories/21172
* SECUNIA: 21174
http://secunia.com/advisories/21174
* SECUNIA: 21399
http://secunia.com/advisories/21399
* SECUNIA: 21478
http://secunia.com/advisories/21478
* SECUNIA: 21848
http://secunia.com/advisories/21848
* SECUNIA: 21598
http://secunia.com/advisories/21598
* SECUNIA: 21744
http://secunia.com/advisories/21744
* SECUNIA: 21986
http://secunia.com/advisories/21986
* SECUNIA: 22140
http://secunia.com/advisories/22140
* SECUNIA: 22317
http://secunia.com/advisories/22317
* SECUNIA: 22523
http://secunia.com/advisories/22523

* SECUNIA: 28749
http://secunia.com/advisories/28749
* SECUNIA: 29640
http://secunia.com/advisories/29640
* SREASON: 1294
http://securityreason.com/securityalert/1294

CVE Reference:

CVE-2006-3918 (cve.mitre.org, nvd.nist.gov)

- **18031 Apache, mod_rewrite off-by-one error**

An off-by-one flaw exists in the Rewrite module, mod_rewrite. Depending on the manner in which Apache httpd was compiled, this software defect may result in a vulnerability which, in combination with certain types of Rewrite rules in the web server configuration files, could be triggered remotely. For vulnerable builds, the nature of the vulnerability can be denial of service (crashing of web server processes) or potentially allow arbitrary code execution.

The vulnerability has been confirmed in Apache 1.3.x up to 1.3.36, 2.0.x up to 2.0.58, 2.2.x up to 2.2.2.

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

References:

* BUGTRAQ: 20060728 Apache mod_rewrite Buffer Overflow Vulnerability
http://www.securityfocus.com/archive/1/archive/1/441487/100/0/threaded
* BUGTRAQ: 20060728 [Announcement] Apache HTTP Server 2.2.3 (2.0.59, 1.3.37) Released
http://www.securityfocus.com/archive/1/archive/1/441485/100/0/threaded
* BUGTRAQ: 20060728 rPSA-2006-0139-1 httpd mod_ssl
http://www.securityfocus.com/archive/1/archive/1/441526/100/200/threaded
* BUGTRAQ: 20060820 POC & exploit for Apache mod_rewrite off-by-one
http://www.securityfocus.com/archive/1/archive/1/443870/100/0/threaded
* FULLDISC: 20060728 Apache 1.3.29/2.X mod_rewrite Buffer Overflow Vulnerability CVE-2006-3747
http://lists.grok.org.uk/pipermail/full-disclosure/2006-July/048267.html
* FULLDISC: 20060728 [Announcement] Apache HTTP Server 2.2.3 (2.0.59, 1.3.37) Released
http://lists.grok.org.uk/pipermail/full-disclosure/2006-July/048271.html
* MISC:
http://kbase.redhat.com/faq/FAQ_68_8653.shtm
* MISC:
http://svn.apache.org/viewvc?view=rev&revision=426144
* CONFIRM:
http://www.apache.org/dist/httpd/Announcement2.0.html
* CONFIRM:
https://issues.rpath.com/browse/RPL-538
* CONFIRM:
http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd?mode=18&ID=3117

* CONFIRM:
http://www-1.ibm.com/support/docview.wss?uid=swg27007951
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=307562
* APPLE: APPLE-SA-2008-03-18
http://lists.apple.com/archives/security-announce/2008/Mar/msg00001.html
* APPLE: APPLE-SA-2008-05-28
http://lists.apple.com/archives/security-announce/2008//May/msg00001.html
* HP: HPSBMA02250
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01118771
* HP: HPSBMA02328
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01428449
* CERT: TA08-150A
http://www.us-cert.gov/cas/techalerts/TA08-150A.html
* CERT-VN: VU#395412
http://www.kb.cert.org/vuls/id/395412
* AIXAPAR: PK27875
http://www-1.ibm.com/support/docview.wss?uid=swg24013080
* AIXAPAR: PK29154
http://www-1.ibm.com/support/docview.wss?uid=swg1PK29154
* AIXAPAR: PK29156
http://www-1.ibm.com/support/docview.wss?uid=swg1PK29156
* DEBIAN: DSA-1131
http://www.debian.org/security/2006/dsa-1131
* DEBIAN: DSA-1132
http://www.debian.org/security/2006/dsa-1132
* GENTOO: GLSA-200608-01
http://security.gentoo.org/glsa/glsa-200608-01.xml
* HP: HPSBUX02145
http://www.securityfocus.com/archive/1/archive/1/445206/100/0/threaded
* HP: HPSBUX02164
http://www.securityfocus.com/archive/1/archive/1/450321/100/0/threaded
* MANDRIVA: MDKSA-2006:133
http://www.mandriva.com/security/advisories?name=MDKSA-2006:133
* OPENPKG: OpenPKG-SA-2006.015
http://www.openpkg.org/security/advisories/OpenPKG-SA-2006.015-apache.html
* SUNALERT: 102662
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102662-1
* SUNALERT: 102663
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102663-1
* SUSE: SUSE-SA:2006:043
http://www.novell.com/linux/security/advisories/2006_43_apache.html
* TRUSTIX: 2006-0044
http://lwn.net/Alerts/194228/
* UBUNTU: USN-328-1
http://www.ubuntu.com/usn/usn-328-1
* BID: 19204
http://www.securityfocus.com/bid/19204
* FRSIRT: ADV-2006-3017
http://www.frsirt.com/english/advisories/2006/3017
* FRSIRT: ADV-2006-3264
http://www.frsirt.com/english/advisories/2006/3264
* FRSIRT: ADV-2006-3282

http://www.frsirt.com/english/advisories/2006/3282
* FRSIRT: ADV-2006-3884
http://www.frsirt.com/english/advisories/2006/3884
* FRSIRT: ADV-2006-3995
http://www.frsirt.com/english/advisories/2006/3995
* FRSIRT: ADV-2006-4015
http://www.frsirt.com/english/advisories/2006/4015
* FRSIRT: ADV-2006-4207
http://www.frsirt.com/english/advisories/2006/4207
* FRSIRT: ADV-2006-4300
http://www.frsirt.com/english/advisories/2006/4300
* FRSIRT: ADV-2006-4868
http://www.frsirt.com/english/advisories/2006/4868
* FRSIRT: ADV-2007-2783
http://www.frsirt.com/english/advisories/2007/2783
* FRSIRT: ADV-2008-0924
http://www.frsirt.com/english/advisories/2008/0924/references
* FRSIRT: ADV-2008-1246
http://www.frsirt.com/english/advisories/2008/1246/references
* FRSIRT: ADV-2008-1697
http://www.frsirt.com/english/advisories/2008/1697
* OSVDB: 27588
http://www.osvdb.org/27588
* SECTRACK: 1016601
http://securitytracker.com/id?1016601
* SECUNIA: 21197
http://secunia.com/advisories/21197
* SECUNIA: 21241
http://secunia.com/advisories/21241
* SECUNIA: 21245
http://secunia.com/advisories/21245
* SECUNIA: 21266
http://secunia.com/advisories/21266
* SECUNIA: 21273
http://secunia.com/advisories/21273
* SECUNIA: 21284
http://secunia.com/advisories/21284
* SECUNIA: 21313
http://secunia.com/advisories/21313
* SECUNIA: 21307
http://secunia.com/advisories/21307
* SECUNIA: 21315
http://secunia.com/advisories/21315
* SECUNIA: 21247
http://secunia.com/advisories/21247
* SECUNIA: 21478
http://secunia.com/advisories/21478
* SECUNIA: 21509
http://secunia.com/advisories/21509
* SECUNIA: 22262
http://secunia.com/advisories/22262
* SECUNIA: 22368
http://secunia.com/advisories/22368
* SECUNIA: 22388
http://secunia.com/advisories/22388

* SECUNIA: 22523
http://secunia.com/advisories/22523
* SECUNIA: 23028
http://secunia.com/advisories/23028
* SECUNIA: 23260
http://secunia.com/advisories/23260
* SECUNIA: 21346
http://secunia.com/advisories/21346
* SECUNIA: 26329
http://secunia.com/advisories/26329
* SECUNIA: 29420
http://secunia.com/advisories/29420

CVE Reference:

CVE-2006-3747 (cve.mitre.org, nvd.nist.gov)

- **18032 Apache, mod_include overflow Vulnerability**

A buffer overflow in mod_include could allow a local user who is authorized to create server side include (SSI) files to gain the privileges of a httpd child.

The vulnerability has been confirmed in Apache 1.3.x up to 1.3.32.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* CONFIRM:
http://support.avaya.com/elmodocs2/security/ASA-2006-081.htm
* DEBIAN: DSA-594
http://www.debian.org/security/2004/dsa-594
* MANDRAKE: MDKSA-2004:134
http://www.mandriva.com/security/advisories?name=MDKSA-2004:134
* REDHAT: RHSA-2004:600
http://www.redhat.com/support/errata/RHSA-2004-600.html
* OPENPKG: OpenPKG-SA-2004.047
http://marc.theaimsgroup.com/?l=bugtraq&m=109906660225051&w=2
* CONFIRM:
http://www.apacheweek.com/features/security-13
* REDHAT: RHSA-2005:816
http://www.redhat.com/support/errata/RHSA-2005-816.html
* SUNALERT: 102197
http://sunsolve.sun.com/search/document.do?assetkey=1-26-102197-1
* BID: 11471
http://www.securityfocus.com/bid/11471
* FRSIRT: ADV-2006-0789
http://www.frsirt.com/english/advisories/2006/0789
* SECTRACK: 1011783
http://securitytracker.com/id?1011783
* SECUNIA: 12898
http://secunia.com/advisories/12898/
* SECUNIA: 19073

http://secunia.com/advisories/19073
* XF: apache-modinclude-bo(17785)
http://xforce.iss.net/xforce/xfdb/17785

CVE Reference:

CVE-2004-0940 (cve.mitre.org, nvd.nist.gov)

- **18033 Apache, mod_digest nonce checking Vulnerability**

mod_digest does not properly verify the nonce of a client response by using a AuthNonce secret. This could allow a malicious user who is able to sniff network traffic to conduct a replay attack against a website using Digest protection. Note that mod_digest implements an older version of the MD5 Digest Authentication specification which is known not to work with modern browsers. This issue does not affect mod_auth_digest.

The vulnerability has been confirmed in Apache 1.3.x up to 1.3.29.

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

References:

* CONFIRM:
http://www.mail-archive.com/dev@httpd.apache.org/msg19007.html
* CONFIRM:
http://www.mail-archive.com/dev@httpd.apache.org/msg19014.html
* MANDRAKE: MDKSA-2004:046
http://www.mandriva.com/security/advisories?name=MDKSA-2004:046
* REDHAT: RHSA-2004:600
http://www.redhat.com/support/errata/RHSA-2004-600.html
* REDHAT: RHSA-2005:816
http://www.redhat.com/support/errata/RHSA-2005-816.html
* SLACKWARE: SSA:2004-133
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.529643
* SUNALERT: 57628
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57628-1
* SUNALERT: 101555
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101555-1
* SUNALERT: 101841
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101841-1
* TRUSTIX: 2004-0027
http://www.trustix.org/errata/2004/0027
* BUGTRAQ: 20040512 [OpenPKG-SA-2004.021] OpenPKG Security Advisory (apache)
http://marc.theaimsgroup.com/?l=bugtraq&m=108437852004207&w=2
* GENTOO: GLSA-200405-22
http://security.gentoo.org/glsa/glsa-200405-22.xml
* BID: 9571
http://www.securityfocus.com/bid/9571
* OVAL: oval:org.mitre.oval:def:4416
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4416

* OVAL: oval:org.mitre.oval:def:100108
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:100108
* SECTRACK: 1008920
http://securitytracker.com/id?1008920
* XF: apache-moddigest-response-replay(15041)
http://xforce.iss.net/xforce/xfdb/15041

CVE Reference:

CVE-2003-0987 (cve.mitre.org, nvd.nist.gov)

- **18034 Apache, Allow/Deny parsing on big-endian 64-bit platforms**

A bug in the parsing of Allow/Deny rules using IP addresses without a netmask on big-endian 64-bit platforms causes the rules to fail to match.

The vulnerability has been confirmed in Apache 1.3.x up to 1.3.29.

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

References:

* CONFIRM:
http://issues.apache.org/bugzilla/show_bug.cgi?id=23850
* MLIST: [apache-cvs] 20040307 cvs commit: apache-1.3/src/modules/standard mod_access.c
http://marc.theaimsgroup.com/?l=apache-cvs&m=107869603013722
* CONFIRM:
http://www.apacheweek.com/features/security-13
* GENTOO: GLSA-200405-22
http://security.gentoo.org/glsa/glsa-200405-22.xml
* MANDRAKE: MDKSA-2004:046
http://frontal2.mandriva.com/security/advisories?name=MDKSA-2004:046
* SLACKWARE: SSA:2004-133
http://www.slackware.com/security/viewer.php?l=slackware-security&y=2004&m=slackware-security.529643
* SUNALERT: 57628
http://sunsolve.sun.com/search/document.do?assetkey=1-26-57628-1
* SUNALERT: 101555
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101555-1
* SUNALERT: 101841
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101841-1
* TRUSTIX: 2004-0027
http://www.trustix.org/errata/2004/0027
* BUGTRAQ: 20040512 [OpenPKG-SA-2004.021] OpenPKG Security Advisory (apache)
http://marc.theaimsgroup.com/?l=bugtraq&m=108437852004207&w=2
* BID: 9829
http://www.securityfocus.com/bid/9829
* OVAL: oval:org.mitre.oval:def:4670
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:4670
* OVAL: oval:org.mitre.oval:def:100111
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:100111

* XF: apache-modaccess-obtain-information(15422)
http://xforce.iss.net/xforce/xfdb/15422

CVE Reference:

CVE-2003-0993 (cve.mitre.org, nvd.nist.gov)

- **18035 Apache, Local configuration regular expression overflow Vulnerability**

By using a regular expression with more than 9 captures a buffer overflow can occur in mod_alias or mod_rewrite. To exploit this an attacker would need to be able to create a carefully crafted configuration file (.htaccess or httpd.conf).

The vulnerability has been confirmed in Apache 1.3.x up to 1.3.28, and 2.0.x up to 2.0.47.

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

References:

* CONFIRM:
http://httpd.apache.org/dist/httpd/Announcement2.html
* APPLE: APPLE-SA-2004-01-26
http://lists.apple.com/archives/security-announce/2004/Jan/msg00000.html
* BUGTRAQ: 20031028 [OpenPKG-SA-2003.046] OpenPKG Security Advisory (apache)
http://www.securityfocus.com/archive/1/342674
* BUGTRAQ: 20031031 GLSA: apache (200310-04)
http://marc.theaimsgroup.com/?l=bugtraq&m=106761802305141&w=2
* HP: HPSBUX0311-301
http://www.securityfocus.com/advisories/6079
* REDHAT: RHSA-2003:320
http://www.redhat.com/support/errata/RHSA-2003-320.html
* REDHAT: RHSA-2003:360
http://www.redhat.com/support/errata/RHSA-2003-360.html
* REDHAT: RHSA-2003:405
http://www.redhat.com/support/errata/RHSA-2003-405.html
* REDHAT: RHSA-2004:015
http://www.redhat.com/support/errata/RHSA-2004-015.html
* REDHAT: RHSA-2005:816
http://www.redhat.com/support/errata/RHSA-2005-816.html
* SCO: SCOSA-2004.6
ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2004.6/SCOSA-2004.6.txt
* SGI: 20031203-01-U
ftp://patches.sgi.com/support/free/security/advisories/20031203-01-U.asc
* CONFIRM:
http://docs.info.apple.com/article.html?artnum=61798
* SGI: 20040202-01-U
ftp://patches.sgi.com/support/free/security/advisories/20040202-01-U.asc
* SUNALERT: 101444
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101444-1
* SUNALERT: 101841
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101841-1

* CERT-VN: VU#434566
http://www.kb.cert.org/vuls/id/434566
* CERT-VN: VU#549142
http://www.kb.cert.org/vuls/id/549142
* BID: 8911
http://www.securityfocus.com/bid/8911
* BID: 9504
http://www.securityfocus.com/bid/9504
* OVAL: oval:org.mitre.oval:def:863
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:863
* OVAL: oval:org.mitre.oval:def:864
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:864
* OVAL: oval:org.mitre.oval:def:3799
http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:3799
* SECUNIA: 10096
http://secunia.com/advisories/10096
* SECUNIA: 10098
http://secunia.com/advisories/10098
* SECUNIA: 10102
http://secunia.com/advisories/10102
* SECUNIA: 10112
http://secunia.com/advisories/10112
* SECUNIA: 10114
http://secunia.com/advisories/10114
* SECUNIA: 10153
http://secunia.com/advisories/10153
* SECUNIA: 10260
http://secunia.com/advisories/10260
* SECUNIA: 10264
http://secunia.com/advisories/10264
* SECUNIA: 10463
http://secunia.com/advisories/10463
* SECUNIA: 10580
http://secunia.com/advisories/10580
* SECUNIA: 10593
http://secunia.com/advisories/10593
* XF: apache-modalias-modrewrite-bo(13400)
http://xforce.iss.net/xforce/xfdb/13400

CVE Reference:

CVE-2003-0542 (cve.mitre.org, nvd.nist.gov)

- **18036 Apache, Rewrite rules that include references allow access to any file**

The Rewrite module, mod_rewrite, can allow access to any file on the web server. The vulnerability occurs only with certain specific cases of using regular expression references in RewriteRule directives: If the destination of a RewriteRule contains regular expression references then an attacker will be able to access any file on the server.

The vulnerability has been confirmed in Apache 1.3.x up to 1.3.12.

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

References:

* BUGTRAQ: 20000929 Security vulnerability in Apache mod_rewrite
http://archives.neohapsis.com/archives/bugtraq/2000-09/0352.html
* REDHAT: RHSA-2000:088
http://www.redhat.com/support/errata/RHSA-2000-088.html
* REDHAT: RHSA-2000:095
http://www.redhat.com/support/errata/RHSA-2000-095.html
* CALDERA: CSSA-2000-035.0
http://www.calderasystems.com/support/security/advisories/CSSA-2000-035.0.txt
* HP: HPSBUX0010-126
http://archives.neohapsis.com/archives/hp/2000-q4/0021.html
* BUGTRAQ: 20001011 Conectiva Linux Security Announcement - apache
http://archives.neohapsis.com/archives/bugtraq/2000-10/0174.html
* BID: 1728
http://www.securityfocus.com/bid/1728
* XF: apache-rewrite-view-files
http://xforce.iss.net/xforce/xfdb/5310

CVE Reference:

CVE-2000-0913 (cve.mitre.org, nvd.nist.gov)

- **18037 Apache, large number of MIME headers Denial of Service Vulnerability**

Apache allows remote attackers to conduct a denial of service via a large number of MIME headers.

The vulnerability has been confirmed in Apache 1.2.x up to 1.2.5, and 1.3.x up to 1.3.1.

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

References:

* BUGTRAQ: 19990903 Web servers / possible DOS Attack / mime header flooding
http://archives.neohapsis.com/archives/bugtraq/1998_3/0742.html

CVE Reference:

CVE-1999-0926 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

- **CVE-2008-1667 HP CVSS 2.0 Score = 7.8**

The Probe Builder Service (aka PBOVISServer.exe) in European Performance Systems (EPS) Probe Builder 2.2 before A.02.20.901, as used in HP OpenView Internet Services (OVIS) on Windows, allows remote attackers to kill arbitrary processes via a process ID number in an unspecified opcode.

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

References:

IDEFENSE: http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=728

HP: http://marc.info/?l=bugtraq&m=121726629109585&w=2

BID: http://www.securityfocus.com/bid/30403

SECUNIA: http://secunia.com/advisories/31278

SECUNIA: http://secunia.com/advisories/31282

CVE Reference: CVE-2008-1667

- **CVE-2008-3364 Trend Micro CVSS 2.0 Score = 9.3**

Buffer overflow in the ObjRemoveCtrl Class ActiveX control in OfficeScanRemoveCtrl.dll 7.3.0.1020 in Trend Micro OfficeScan Corp Edition Web-Deployment 7.3 build 1343 Patch 4 allows remote attackers to execute arbitrary code via a long string in the Server property, and possibly other properties. NOTE: some of these details are obtained from third party information.

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

References:

MILW0RM: http://www.milw0rm.com/exploits/6152

BID: http://www.securityfocus.com/bid/30407

FRSIRT: http://www.frsirt.com/english/advisories/2008/2220/references

SECUNIA: http://secunia.com/advisories/31277

XF: http://xforce.iss.net/xforce/xfdb/44042

CVE Reference: CVE-2008-3364

- **CVE-2008-3373 Grisoft CVSS 2.0 Score = 5.0**

The files parsing engine in Grisoft AVG Anti-Virus before 8.0.156 allows remote attackers to cause a denial of service (engine crash) via a crafted UPX compressed file, which triggers a divide-by-zero error.

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

References:

http://www.nruns.com/advisories/%5Bn.runs-SA-2008%20004%5D%20-%20AVG%20Antivirus%20UPX%20parsing%20Divide%20by%20Zero%20Advisory.txt

http://www.grisoft.com/ww.94247

BID: http://www.securityfocus.com/bid/30417

SECUNIA: http://secunia.com/advisories/31290

CVE Reference: CVE-2008-3373

- **CVE-2008-3330 Debian CVSS 2.0 Score = 4.3**

Cross-site scripting (XSS) vulnerability in services/obrowser/index.php in Horde 3.2 and Turba 2.2 allows remote attackers to inject arbitrary web script or HTML via the contact name.

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

References:

http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=492578

CVE Reference: CVE-2008-3330

- **CVE-2008-3323 redhat CVSS 2.0 Score = 10.0**

setup.exe before 2.573.2.3 in Cygwin does not properly verify the authenticity of packages, which allows remote Cygwin mirror servers or man-in-the-middle attackers to execute arbitrary code via a package list containing the MD5 checksum of a Trojan horse package.

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

References:

BUGTRAQ:
http://www.securityfocus.com/archive/1/archive/1/494756/100/0/threaded

http://www.security-objectives.com/advisories/SECOBJADV-2008-02.txt

https://bugzilla.redhat.com/show_bug.cgi?id=449929

CVE Reference: CVE-2008-3323

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