

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://www2.netvigilance.com/productdownloads?productname=apachechunkedvulnerabilityscanner>

This Week in Review

Digital spies. Arrests in \$14M cyber scam. Occupy occupying mayor's email. This week's ssl certificate authority disaster.

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

• Adversaries, allies stealing U.S. trade secrets

Foreign spies, including U.S. allies, are increasingly launching digital assaults against the nation to steal sensitive economic secrets, according to a report issued Thursday by the U.S. Office of National Counterintelligence Executive (UNSEX). The report, which UNSEX prepares for Congress every two years, details industrial espionage and economic information and technology theft between 2009 and 2011. China and Russia were specifically called out as the world's most prolific perpetrators of economic espionage against the United States.

Both countries view themselves as strategic competitors of America, and they carry out such activities to support their own economic development and security, according to the report, compiled with input from at least 13 other U.S. intelligence agencies. SC Magazine

Full Story :

http://www.scmagazineus.com/adversaries-allies-stealing-us-trade-secrets/article/216200/?utm_source=feedburner&

• FBI arrests six in click-fraud cyber scam that netted \$14M

Six men believed to be behind a massive click-fraud scheme were arrested on Monday following a two-year, international police investigation, dubbed Operation Ghost Click, the FBI announced Wednesday.

The racket led to the infection of more than four million computers in 100 countries with malware.

The defendants, all of whom are Estonian nationals, were arrested in their native country. The U.S. attorney's office is planning to seek their extradition to the United States. The seventh defendant, a Russian national, remains at large. SC Magazine

Full Story :

http://www.scmagazineus.com/fbi-arrests-six-in-click-fraud-cyber-scam-that-netted-14m/article/216399/?utm_source=

• **Occupy St. Louis sympathizer hacks mayor's website**

A person supportive of the Occupy Wall Street movements sweeping the nation has hacked into the website belonging to the St. Louis mayor, defacing it and publicly exposing contact information and emails.

The hacker, apparently affiliated with the Anonymous online collective, dumped the contact details of hundreds of Mayor Francis Slay's political supporters, in addition to 2,000 emails sent by Slay since he became mayor in 2001, according to a Reuters report. The stolen information was posted in a Pastebin document, which since has been removed.

The site -- www.mayorslay.com -- also was defaced to include the all-capitalized message: "You can remove the movement from the city, but you cannot remove the movement from your systems!" SC Magazine

Full Story :

http://www.scmagazineus.com/occupy-st-louis-sympathizer-hacks-mayors-website/article/216510/?utm_source=feedb

• **Another Dutch certificate authority halts business**

Another Dutch-based SSL certificate authority has stopped issuing credentials following a security incident.

KPN Corporate Market, one of the Netherlands largest telecommunications and IT service providers, announced Friday in a news release (translated) that it has temporarily halted the issuance of certificates, pending an additional investigation. Already issued certs, however, remain valid.

A recent examination of a web server turned up "abuse" that may have happened up to four years ago, the company said. Hackers may have wanted to use the server to launch distributed denial-of-service attacks against their targets. SC Magazine

Full Story :

http://www.scmagazineus.com/another-dutch-certificate-authority-halts-business/article/216217/?utm_source=feedb

New Vulnerabilities Tested in SecureScout

• **13826 Oracle Database Server - Core RDBMS component SQL Injection Vulnerability (oct-2011/CVE-2011-3512)**

Oracle Database is prone to an SQL-injection vulnerability.

A successful exploit may allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

Oracle Database supports spatial datatypes. A vulnerability exists in the handling of spatial indexes. Users with create table and create procedure privileges can elevate their privileges to SYSDBA

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

References:

* CONFIRM:

<http://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html>

* MISC:

<http://www.teamshatter.com/topics/general/team-shatter-exclusive/sql-injection-vulnerability-in-oracle-drop-index-for-spatial>

* MISC:

<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3512>

CVE Reference:

CVE-2011-3512 (cve.mitre.org, nvd.nist.gov)

• 19565 Apache APR 'apr_fnmatch()' Denial of Service Vulnerability

Apache APR is prone to a vulnerability that may allow attackers to cause a denial-of-service condition.

Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via `*?` sequences in the first argument, as demonstrated by attacks against `mod_autoindex` in `httpd`.

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

References:

- * SREASONRES: 20110512 Multiple Vendors libc/fnmatch(3) DoS (incl apache)
http://securityreason.com/achievement_securityalert/98
- * MLIST: [dev] 20110510 Re: Apache Portable Runtime 1.4.4 [...] Released
<http://www.mail-archive.com/dev@apr.apache.org/msg23961.html>
- * MLIST: [dev] 20110510 Re: fnmatch rewrite in apr, apr 1.4.3
<http://www.mail-archive.com/dev@apr.apache.org/msg23960.html>
- * MLIST: [dev] 20110511 Re: Apache Portable Runtime 1.4.4 [...] Released
<http://www.mail-archive.com/dev@apr.apache.org/msg23976.html>
- * MISC:
<http://cxib.net/stuff/apache.fnmatch.phps>
- * CONFIRM:
<http://cvsweb.netbsd.org/bsdweb.cgi/src/lib/libc/gen/fnmatch.c#rev1.22>
- * CONFIRM:
http://httpd.apache.org/security/vulnerabilities_22.html
- * CONFIRM:
http://svn.apache.org/viewvc/apr/apr/branches/1.4.x/strings/apr_fnmatch.c?r1=731029&r2=1098902
- * CONFIRM:
<http://svn.apache.org/viewvc?view=revision&revision=1098188>
- * CONFIRM:
<http://svn.apache.org/viewvc?view=revision&revision=1098799>
- * CONFIRM:
<http://www.apache.org/dist/apr/Announcement1.x.html>
- * CONFIRM:
<http://www.apache.org/dist/apr/CHANGES-APR-1.4>
- * CONFIRM:
<http://www.apache.org/dist/httpd/Announcement2.2.html>
- * CONFIRM:
<http://www.openbsd.org/cgi-bin/cvsweb/src/lib/libc/gen/fnmatch.c#rev1.15>
- * CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=703390
- * CONFIRM:
<http://support.apple.com/kb/HT5002>
- * APPLE: APPLE-SA-2011-10-12-3
<http://lists.apple.com/archives/Security-announce/2011/Oct/msg00003.html>
- * DEBIAN: DSA-2237
<http://www.debian.org/security/2011/dsa-2237>
- * HP: HPSBUX02702
<http://marc.info/?l=bugtraq&m=131551295528105&w=2>
- * HP: HPSBUX02707
<http://marc.info/?l=bugtraq&m=131731002122529&w=2>
- * MANDRIVA: MDVSA-2011:084
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:084>
- * REDHAT: RHSA-2011:0507
<http://www.redhat.com/support/errata/RHSA-2011-0507.html>
- * REDHAT: RHSA-2011:0896
<http://www.redhat.com/support/errata/RHSA-2011-0896.html>
- * REDHAT: RHSA-2011:0897
<http://www.redhat.com/support/errata/RHSA-2011-0897.html>
- * SECTRACK: 1025527
<http://securitytracker.com/id?1025527>
- * SECUNIA: 44490
<http://secunia.com/advisories/44490>
- * SECUNIA: 44564
<http://secunia.com/advisories/44564>
- * SECUNIA: 44574
<http://secunia.com/advisories/44574>

* SREASON: 8246

<http://securityreason.com/securityalert/8246>

CVE Reference:

CVE-2011-0419 (cve.mitre.org, nvd.nist.gov)

• 19566 Apple QuickTime Pict File Handling Integer Overflow Vulnerability

Apple QuickTime before 7.7.1 is prone to an Integer overflow on Windows which may allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted PICT file.

The problem occurs when handling a specially crafted PICT image file. Successful exploits may allow attackers to execute arbitrary code in the context of the currently logged-in user; failed exploit attempts may cause denial-of-service conditions.

Versions prior to QuickTime 7.7.1 are vulnerable on Windows 7, Vista, XP, and Mac OS X platforms.

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

References:

* CONFIRM:

<http://support.apple.com/kb/HT5016>

* BID: 50399

<http://www.securityfocus.com/bid/50399/info>

* MISC: CVE-2011-3247

<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3247>

CVE Reference:

CVE-2011-3247 (cve.mitre.org, nvd.nist.gov)

• 19567 Apple QuickTime QTVR File Memory Corruption Remote Code Execution Vulnerability

Apple QuickTime is prone to a remote code-execution vulnerability because of a memory-corruption error.

Integer signedness error in Apple QuickTime before 7.6.9 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted panorama atom in a QuickTime Virtual Reality (QTVR) movie file.

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

References:

* MISC:

<http://zerodayinitiative.com/advisories/ZDI-10-260/>

* CONFIRM:

<http://support.apple.com/kb/HT4447>

* CONFIRM:

<http://support.apple.com/kb/HT4581>

* APPLE: APPLE-SA-2010-12-07-1

<http://lists.apple.com/archives/security-announce/2010/Dec/msg00000.html>

* APPLE: APPLE-SA-2011-03-21-1

<http://lists.apple.com/archives/security-announce/2011/Mar/msg00006.html>

* OSVDB: 69756

<http://osvdb.org/69756>

* SECTRACK: 1024830

<http://www.securitytracker.com/id?1024830>

* BID: 45239

<http://www.securityfocus.com/bid/45239/info>

CVE Reference:

CVE-2010-3802 (cve.mitre.org, nvd.nist.gov)

• 19568 PHP 'Zip' Extension 'zip_fread()' Function Denial of Service Vulnerability

PHP is prone to a remote denial-of-service vulnerability that affects the 'Zip' extension.

Integer signedness error in zip_stream.c in the Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (CPU consumption) via a malformed archive file that triggers errors in zip_fread function calls.

Successful attacks will cause the application to crash, creating a denial-of-service condition. Due to the nature of this

issue, arbitrary code-execution may be possible; however, this has not been confirmed.

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

References:

- * CONFIRM:
<http://bugs.php.net/bug.php?id=49072>
- * CONFIRM:
<http://www.php.net/ChangeLog-5.php>
- * CONFIRM:
<http://support.apple.com/kb/HT5002>
- * APPLE: APPLE-SA-2011-10-12-3
<http://lists.apple.com/archives/Security-announce/2011/Oct/msg00003.html>
- * DEBIAN: DSA-2266
<http://www.debian.org/security/2011/dsa-2266>
- * MANDRIVA: MDVSA-2011:052
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:052>
- * MANDRIVA: MDVSA-2011:053
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:053>
- * BID: 46975
<http://www.securityfocus.com/bid/46975>
- * VUPEN: ADV-2011-0744
<http://www.vupen.com/english/advisories/2011/0744>

CVE Reference:

CVE-2011-1471 (cve.mitre.org, nvd.nist.gov)

• 19569 PHP Calendar Extension 'SdnToJulian()' Remote Integer Overflow Vulnerability

PHP is prone to an integer-overflow vulnerability in the calendar extension because it fails to ensure that integer values are not overrun.

Integer overflow in the SdnToJulian function in the Calendar extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a large integer in the first argument to the cal_from_jd function.

Successful exploits of this vulnerability allow remote attackers to execute arbitrary code in the context of a webserver affected by the issue. Failed attempts will likely result in denial-of-service conditions.

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

References:

- * CONFIRM:
<http://bugs.php.net/bug.php?id=53574>
- * CONFIRM:
<http://www.php.net/ChangeLog-5.php>
- * CONFIRM:
<http://support.apple.com/kb/HT5002>
- * APPLE: APPLE-SA-2011-10-12-3
<http://lists.apple.com/archives/Security-announce/2011/Oct/msg00003.html>
- * DEBIAN: DSA-2266
<http://www.debian.org/security/2011/dsa-2266>
- * MANDRIVA: MDVSA-2011:052
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:052>
- * MANDRIVA: MDVSA-2011:053
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:053>
- * BID: 46967
<http://www.securityfocus.com/bid/46967>
- * VUPEN: ADV-2011-0744
<http://www.vupen.com/english/advisories/2011/0744>

CVE Reference:

CVE-2011-1466 (cve.mitre.org, nvd.nist.gov)

• 19570 PHP Security Bypass Vulnerability

PHP is prone to a security-bypass vulnerability.

The rfc1867_post_handler function in main/rfc1867.c in PHP before 5.3.7 does not properly restrict filenames in

multipart/form-data POST requests, which allows remote attackers to conduct absolute path traversal attacks, and possibly create or overwrite arbitrary files, via a crafted upload request, related to a "file path injection vulnerability."

Successful exploits will allow an attacker to create arbitrary files from the root directory, which may aid in further attacks.

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

References:

- * MLIST: [oss-security] 20110612 CVE Request: PHP File upload filename
<http://openwall.com/lists/oss-security/2011/06/12/5>
- * MLIST: [oss-security] 20110613 Re: CVE Request: PHP File upload filename
<http://openwall.com/lists/oss-security/2011/06/13/15>
- * MISC:
<http://pastebin.com/1edSuSVN>
- * CONFIRM:
<http://bugs.php.net/bug.php?id=54939>
- * CONFIRM:
http://svn.php.net/viewvc/php/php-src/branches/PHP_5_3/NEWS?view=markup&pathrev=312103
- * CONFIRM:
http://svn.php.net/viewvc/php/php-src/branches/PHP_5_3/main/rfc1867.c?r1=312103&r2=312102&pathrev=312103
- * CONFIRM:
<http://svn.php.net/viewvc?view=revision&revision=312103>
- * CONFIRM:
<http://www.php.net/ChangeLog-5.php#5.3.7>
- * CONFIRM:
<http://www.php.net/archive/2011.php#id2011-08-18-1>
- * DEBIAN: DSA-2266
<http://www.debian.org/security/2011/dsa-2266>
- * BID: 48259
<http://www.securityfocus.com/bid/48259>
- * BID: 49241
<http://www.securityfocus.com/bid/49241>
- * SECTRACK: 1025659
<http://securitytracker.com/id?1025659>
- * SECUNIA: 44874
<http://secunia.com/advisories/44874>
- * XF: php-sapiposthandlerfunc-sec-bypass(67999)
<http://xforce.iss.net/xforce/xfdb/67999>

CVE Reference:

CVE-2011-2202 (cve.mitre.org, nvd.nist.gov)

• 19571 VMware Hosted Products UDF File Systems Buffer Overflow Vulnerability

Buffer overflow in VMware Workstation 7.x before 7.1.5 allows remote attackers to execute arbitrary code via a crafted UDF filesystem in an ISO image.

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

References:

- * BUGTRAQ: 20111005 VMSA-2011-0011 VMware hosted products address remote code execution vulnerability
<http://www.securityfocus.com/archive/1/archive/1/520005/100/0/threaded>
- * CONFIRM:
<http://www.vmware.com/security/advisories/VMSA-2011-0011.html>
- * BID: 49942
<http://www.securityfocus.com/bid/49942>
- * OSVDB: 76060
<http://osvdb.org/76060>
- * SECTRACK: 1026139
<http://www.securitytracker.com/id?1026139>
- * SECUNIA: 46241
<http://secunia.com/advisories/46241>

CVE Reference:

CVE-2011-3868 (cve.mitre.org, nvd.nist.gov)

• 19572 Apache HTTP Server 'mod_proxy' Reverse Proxy Information Disclosure Vulnerability

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.

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

References:

- * EXPLOIT-DB: 17969
<http://www.exploit-db.com/exploits/17969>
- * FULLDISC: 20111005 Apache HTTP Server: mod_proxy reverse proxy exposure (CVE-2011-3368)
<http://seclists.org/fulldisclosure/2011/Oct/232>
- * MLIST: [announce] 20111005 Advisory: mod_proxy reverse proxy exposure (CVE-2011-3368)
<http://web.archiveorange.com/archive/v/ZyS0hzECD5zzb2NkvQlt>
- * MISC:
<http://www.contextis.com/research/blog/reverseproxybypass/>
- * CONFIRM:
<http://svn.apache.org/viewvc?view=revision&revision=1179239>
- * CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=740045
- * AIXAPAR: SE49723
<http://www-01.ibm.com/support/docview.wss?uid=nas2064c7e5f53452ff686257927003c8d42>
- * AIXAPAR: SE49724
<http://www-01.ibm.com/support/docview.wss?uid=nas2b7c57b1f1035675186257927003c8d48>
- * MANDRIVA: MDVSA-2011:144
<http://www.mandriva.com/security/advisories?name=MDVSA-2011:144>
- * REDHAT: RHSA-2011:1391
<http://www.redhat.com/support/errata/RHSA-2011-1391.html>
- * REDHAT: RHSA-2011:1392
<http://www.redhat.com/support/errata/RHSA-2011-1392.html>
- * BID: 49957
<http://www.securityfocus.com/bid/49957>
- * SECTRACK: 1026144
<http://www.securitytracker.com/id?1026144>
- * SECUNIA: 46288
<http://secunia.com/advisories/46288>
- * SECUNIA: 46414
<http://secunia.com/advisories/46414>
- * XF: apache-modproxy-information-disclosure(70336)
<http://xforce.iss.net/xforce/xfdb/70336>

CVE Reference:

CVE-2011-3368 (cve.mitre.org, nvd.nist.gov)

● 19573 PHP Security bug in is_a function allow arbitrary code execution

The is_a function in PHP 5.3.7 and 5.3.8 triggers a call to the __autoload function, which makes it easier for remote attackers to execute arbitrary code by providing a crafted URL and leveraging potentially unsafe behavior in certain PEAR packages and custom autoloaders.

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

References:

- * BUGTRAQ: 20110923 Security issue is_a function in PHP 5.3.7
<http://www.securityfocus.com/archive/1/519770/30/0/threaded>
- * MISC:
http://www.byte.nl/blog/2011/09/23/security-bug-in-is_a-function-in-php-5-3-7-5-3-8/
- * CONFIRM:
<http://svn.php.net/viewvc/?view=revision&revision=317183>
- * CONFIRM:
<https://bugs.php.net/bug.php?id=55475>
- * CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=741020

CVE Reference:

CVE-2011-3379 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2011-2013 Microsoft CVSS 2.0 Score = 10.0

Integer overflow in the TCP/IP implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code by sending a sequence of crafted UDP packets to a closed port, aka "Reference Counter Overflow Vulnerability."

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

References:

MS: <http://technet.microsoft.com/security/bulletin/MS11-083>

CVE Reference: [CVE-2011-2013](#)

• CVE-2011-2016 Microsoft CVSS 2.0 Score = 9.3

Untrusted search path vulnerability in Windows Mail and Windows Meeting Space in Microsoft Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .eml or .wcinv file, aka "Windows Mail 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://technet.microsoft.com/security/bulletin/MS11-085>

CVE Reference: [CVE-2011-2016](#)

• CVE-2011-2014 Microsoft CVSS 2.0 Score = 9.0

The LDAP over SSL (aka LDAPS) implementation in Active Directory, Active Directory Application Mode (ADAM), and Active Directory Lightweight Directory Service (AD LDS) in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not examine Certificate Revocation Lists (CRLs), which allows remote authenticated users to bypass intended certificate restrictions and access Active Directory resources by leveraging a revoked X.509 certificate for a domain account, aka "LDAPS Authentication Bypass Vulnerability."

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

References:

MS: <http://technet.microsoft.com/security/bulletin/MS11-086>

CVE Reference: [CVE-2011-2014](#)

• CVE-2011-2004 Microsoft CVSS 2.0 Score = 7.1

Array index error in win32k.sys in the kernel-mode drivers in Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (reboot) via a crafted TrueType font file, aka "TrueType Font Parsing Vulnerability," a different vulnerability than CVE-2011-3402.

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

References:

MS: <http://technet.microsoft.com/security/bulletin/MS11-084>

CVE Reference: [CVE-2011-2004](#)

• CVE-2011-3607 Apache CVSS 2.0 Score = 4.4

Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.

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

References:

CONFIRM: https://bugzilla.redhat.com/show_bug.cgi?id=750935

CONFIRM: <https://bugs.launchpad.net/ubuntu/+source/apache2/+bug/811422>

XF: <http://xforce.iss.net/xforce/xfdb/71093>

BID: <http://www.securityfocus.com/bid/50494>

OSVDB: <http://www.osvdb.org/76744>

MISC: <http://www.halfdog.net/Security/2011/ApacheModSetEnvIfIntegerOverflow/DemoExploit.html>

MISC: <http://www.halfdog.net/Security/2011/ApacheModSetEnvIfIntegerOverflow/>

SECTRAK: <http://securitytracker.com/id?1026267>

SECUNIA: <http://secunia.com/advisories/45793>

FULLDISC: <http://archives.neohapsis.com/archives/fulldisclosure/2011-11/0023.html>

CVE Reference: [CVE-2011-3607](#)

• **CVE-2011-4415 Apache CVSS 2.0 Score = 4.0**

The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the "len += " statement and (2) the apr_pccalloc function call, a different vulnerability than CVE-2011-3607.

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

References:

MISC: <http://www.halfdog.net/Security/2011/ApacheModSetEnvIfIntegerOverflow/>

MISC: <http://www.halfdog.net/Security/2011/ApacheModSetEnvIfIntegerOverflow/DemoExploit.html>

CONFIRM: <http://www.gossamer-threads.com/lists/apache/dev/403775>

CVE Reference: [CVE-2011-4415](#)

• **CVE-2011-3168 HP CVSS 2.0 Score = 5.0**

Unspecified vulnerability in the POP and IMAP service implementations in HP TCP/IP Services 5.6 and 5.7 for OpenVMS allows remote attackers to obtain sensitive information via unknown vectors.

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

References:

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01908983>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01908983>

CVE Reference: [CVE-2011-3168](#)

• **CVE-2011-3169 HP CVSS 2.0 Score = 5.0**

Unspecified vulnerability in the SMTP service implementation in HP TCP/IP Services 5.6 and 5.7 for OpenVMS allows remote attackers to cause a denial of service via unknown vectors.

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

References:

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01915145>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01915145>

CVE Reference: [CVE-2011-3169](#)

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