

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

[WinHoneyd v1.5c](#) - Download WinHoneyd executable package by filling our download form. Size: 2407KB

Download Here:

<http://www.netvigilance.com/productdownloads?productname=winhoneyd-1.5c.zip>

This Week in Review

Best practices on encryption from Visa. New wave of SQL injections. Huge increase in spamborne malware. The Informed P2P User Act.

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

• Visa creates guidance for merchants wanting to encrypt

Visa on Monday released a best practices document for merchants considering adoption of end-to-end encryption, an emerging technology used to mask cardholder data from point-of-swipe through processing.

The guidance is meant to fill a temporary void until industry standards are established by the American National Standards Institute, Jennifer Fischer, senior business leader in Visa's payment system risk division, told SCMagazineUS.com on Monday.

"We felt it was important to provide [help] for those companies clearly looking for guidance today," she said. "I think a lot of merchants are looking for that next solution that is going to be a longer-term data security step." SC Magazine

Full Story :

<http://www.scmagazineus.com/Visa-creates-guidance-for-merchants-wanting-to-encrypt/article/151556/>

• Asprox botnet launches new wave of SQL injection

The Asprox botnet has laid low for the first half of the year but the cybercriminals behind it again have begun utilizing its network of infected computers to carry out SQL injection attacks against vulnerable websites, security firms are warning.

The latest wave of SQL injection attempts emanating from the Asprox botnet began last Monday, Jason Milletary, counter threat unit security researcher at managed security services vendor SecureWorks, told SCMagazineUS.com on Tuesday.

"Asprox is fairly unsophisticated," Gunter Ollmann, vice president of research at enterprise security firm Damballa, told SCMagazineUS.com on Tuesday. "The SQL injection attacks it tries to launch are unsophisticated - but it works." SC Magazine

Full Story :

<http://www.scmagazineus.com/Asprox-botnet-launches-new-wave-of-SQL-injection/article/151615/>

• Huge uptick in spam-borne malware since mid-September

The amount of spam containing malicious attachments spiked in September and has remained at an elevated level since, according to Symantec's "State of Spam" report released Wednesday.

"We are definitely seeing an increase in spam with attached viruses," Dylan Morss, senior manager of anti-spam engineering for Symantec, told SCMagazineUS.com on Wednesday.

Generally, the amount of spam containing malicious attachments hovers around 0.5 percent of all spam, with occasional brief spikes every two to three months, Morss said. Since mid-September, however, malicious attachments have been present in approximately 1.3 percent of all spam on average. SC Magazine

Full Story :

<http://www.scmagazineus.com/Huge-uptick-in-spam-borne-malware-since-mid-September/article/151732/>

• House weighs bill protecting accidental P2P data leaks

The U.S. House Energy and Commerce Committee has passed a bill intended to prevent inadvertent disclosure of information on peer-to-peer (P2P) file-sharing programs.

The Informed P2P User Act, set forth in March by Reps. Mary Bono Mack, R-Calif., John Barrow, D-Ga., and Joe Barton, R-Texas, would require that users be notified and permitted to consent before they installed P2P client software to make files publicly available. The bill was passed by the Energy and Commerce Committee last Wednesday and it will now go to the full House for approval.

"We are all too familiar with the danger of inadvertent sharing of sensitive information through the use, or misuse, of certain file sharing programs," said Rep. Henry Waxman, D-Calif., chairman of the Committee on Energy and Commerce, during his opening remarks Wednesday. "Tax returns, medical files, and even classified government documents have been found on these networks." SC Magazine

Full Story :

<http://www.scmagazineus.com/House-weighs-bill-protecting-accidental-P2P-data-leaks/article/151563/>

New Vulnerabilities Tested in SecureScout

• 18544 Apache APR-util heap underwrite Vulnerability

A heap-based underwrite flaw was found in the way the bundled copy of the APR-util library created compiled forms of particular search patterns. An attacker could formulate a specially-crafted search keyword, that would overwrite arbitrary heap memory locations when processed by the pattern preparation engine.

The issue is fixed in version 2.2.12.

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

References:

* CONFIRM:

<http://www.apache.org/dist/apr/CHANGES-APR-UTIL-1.3>

* CONFIRM:

https://bugzilla.redhat.com/show_bug.cgi?id=503928

* CONFIRM:

<http://svn.apache.org/viewvc?view=rev&revision=779880>

* AIXAPAR: PK88341

<http://www-01.ibm.com/support/docview.wss?uid=swg1PK88341>

* AIXAPAR: PK91241
<http://www-01.ibm.com/support/docview.wss?uid=swg1PK91241>

* DEBIAN: DSA-1812
<http://www.debian.org/security/2009/dsa-1812>

* FEDORA: FEDORA-2009-5969
<https://www.redhat.com/archives/fedora-package-announce/2009-June/msg01228.html>

* FEDORA: FEDORA-2009-6014
<https://www.redhat.com/archives/fedora-package-announce/2009-June/msg01173.html>

* FEDORA: FEDORA-2009-6261
<https://www.redhat.com/archives/fedora-package-announce/2009-June/msg01201.html>

* GENTOO: GLSA-200907-03
<http://security.gentoo.org/glsa/glsa-200907-03.xml>

* MANDRIVA: MDVSA-2009:131
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:131>

* REDHAT: RHSA-2009:1107
<http://www.redhat.com/support/errata/RHSA-2009-1107.html>

* REDHAT: RHSA-2009:1108
<http://www.redhat.com/support/errata/RHSA-2009-1108.html>

* SLACKWARE: SSA:2009-167-02
<http://slackware.com/security/viewer.php?l=slackware-security&y=2009&m=slackware-security.538210>

* UBUNTU: USN-786-1
<http://www.ubuntu.com/usn/usn-786-1>

* UBUNTU: USN-787-1
<http://www.ubuntu.com/usn/usn-787-1>

* BID: 35221
<http://www.securityfocus.com/bid/35221>

* SECUNIA: 35284
<http://secunia.com/advisories/35284>

* SECUNIA: 35360
<http://secunia.com/advisories/35360>

* SECUNIA: 34724
<http://secunia.com/advisories/34724>

* SECUNIA: 35444
<http://secunia.com/advisories/35444>

* SECUNIA: 35487
<http://secunia.com/advisories/35487>

* SECUNIA: 35395
<http://secunia.com/advisories/35395>

* SECUNIA: 35565
<http://secunia.com/advisories/35565>

* SECUNIA: 35710
<http://secunia.com/advisories/35710>

* SECUNIA: 35843
<http://secunia.com/advisories/35843>

* SECUNIA: 35797
<http://secunia.com/advisories/35797>

* VUPEN: ADV-2009-1907
<http://www.vupen.com/english/advisories/2009/1907>

* XF: apache-aprstrmatchprecompile-dos(50964)
<http://xforce.iss.net/xforce/xfdb/50964>

CVE Reference:

CVE-2009-0023 (cve.mitre.org, nvd.nist.gov)

• 18545 Apache APR-util XML Denial of Service Vulnerability

A denial of service flaw was found in the bundled copy of the APR-util library Extensible Markup Language (XML) parser. A remote attacker could create a specially-crafted XML document that would cause excessive memory consumption when processed by the XML decoding engine.

The issue is fixed in version 2.2.12.

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

References:

* BUGTRAQ: 20090824 rPSA-2009-0123-1 apr-util
<http://www.securityfocus.com/archive/1/archive/1/506053/100/0/threaded>

* MILWORM: 8842
<http://www.milw0rm.com/exploits/8842>

* MLIST: [apr-dev] 20090602 [PATCH] prevent "billion laughs" attack against expat
<http://marc.info/?l=apr-dev&m=124396021826125&w=2>

* MLIST: [oss-security] 20090603 CVE request: "billion laughs" attack against Apache APR
<http://www.openwall.com/lists/oss-security/2009/06/03/4>

* CONFIRM:
<http://svn.apache.org/viewvc?view=rev&revision=781403>

* CONFIRM:
<http://www.apache.org/dist/apr/CHANGES-APR-UTIL-1.3>

* CONFIRM:
<http://wiki.rpath.com/Advisories:rPSA-2009-0123>

* AIXAPAR: PK88342
<http://www-01.ibm.com/support/docview.wss?uid=swg1PK88342>

* AIXAPAR: PK91241
<http://www-01.ibm.com/support/docview.wss?uid=swg1PK91241>

* DEBIAN: DSA-1812
<http://www.debian.org/security/2009/dsa-1812>

* FEDORA: FEDORA-2009-5969
<https://www.redhat.com/archives/fedora-package-announce/2009-June/msg01228.html>

* FEDORA: FEDORA-2009-6014
<https://www.redhat.com/archives/fedora-package-announce/2009-June/msg01173.html>

* FEDORA: FEDORA-2009-6261
<https://www.redhat.com/archives/fedora-package-announce/2009-June/msg01201.html>

* GENTOO: GLSA-200907-03
<http://security.gentoo.org/glsa/glsa-200907-03.xml>

* MANDRIVA: MDVSA-2009:131
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:131>

* REDHAT: RHSA-2009:1107
<http://www.redhat.com/support/errata/RHSA-2009-1107.html>

* REDHAT: RHSA-2009:1108
<http://www.redhat.com/support/errata/RHSA-2009-1108.html>

* SLACKWARE: SSA:2009-167-02
<http://slackware.com/security/viewer.php?l=slackware-security&y=2009&m=slackware-security.538210>

* UBUNTU: USN-786-1
<http://www.ubuntu.com/usn/usn-786-1>

* UBUNTU: USN-787-1
<http://www.ubuntu.com/usn/usn-787-1>

* BID: 35253
<http://www.securityfocus.com/bid/35253>

* SECUNIA: 35284
<http://secunia.com/advisories/35284>

* SECUNIA: 35360
<http://secunia.com/advisories/35360>

* SECUNIA: 34724
<http://secunia.com/advisories/34724>

* SECUNIA: 35444
<http://secunia.com/advisories/35444>

* SECUNIA: 35487
<http://secunia.com/advisories/35487>

* SECUNIA: 35395
<http://secunia.com/advisories/35395>

* SECUNIA: 35565
<http://secunia.com/advisories/35565>

* SECUNIA: 35710
<http://secunia.com/advisories/35710>

* SECUNIA: 35843
<http://secunia.com/advisories/35843>

* SECUNIA: 35797
<http://secunia.com/advisories/35797>

* SECUNIA: 36473
<http://secunia.com/advisories/36473>

* VUPEN: ADV-2009-1907
<http://www.vupen.com/english/advisories/2009/1907>

CVE Reference:

CVE-2009-1955 (cve.mitre.org, nvd.nist.gov)

• 18546 Apache APR-util off-by-one overflow Vulnerability

An off-by-one overflow flaw was found in the way the bundled copy of the APR-util library processed a variable list of arguments. An attacker could provide a specially-crafted string as input for the formatted output conversion routine,

which could, on big-endian platforms, potentially lead to the disclosure of sensitive information or a denial of service.

The issue is fixed in version 2.2.12.

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

References:

- * MLIST: [dev] 20090424 Buffer overflow in apr_brigade_vprintf() ?
<http://www.mail-archive.com/dev@apr.apache.org/msg21591.html>
- * MLIST: [dev] 20090424 Re: Buffer overflow in apr_brigade_vprintf() ?
<http://www.mail-archive.com/dev@apr.apache.org/msg21592.html>
- * MLIST: [oss-security] 20090605 CVE Request (apr-util)
<http://www.openwall.com/lists/oss-security/2009/06/06/1>
- * CONFIRM:
<http://svn.apache.org/viewvc?view=rev&revision=768417>
- * CONFIRM:
<http://www.apache.org/dist/apr/CHANGES-APR-UTIL-1.3>
- * CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=504390
- * AIXAPAR: PK88341
<http://www-01.ibm.com/support/docview.wss?uid=swg1PK88341>
- * AIXAPAR: PK91241
<http://www-01.ibm.com/support/docview.wss?uid=swg1PK91241>
- * FEDORA: FEDORA-2009-5969
<https://www.redhat.com/archives/fedora-package-announce/2009-June/msg01228.html>
- * FEDORA: FEDORA-2009-6014
<https://www.redhat.com/archives/fedora-package-announce/2009-June/msg01173.html>
- * FEDORA: FEDORA-2009-6261
<https://www.redhat.com/archives/fedora-package-announce/2009-June/msg01201.html>
- * GENTOO: GLSA-200907-03
<http://security.gentoo.org/glsa/glsa-200907-03.xml>
- * MANDRIVA: MDVSA-2009:131
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:131>
- * REDHAT: RHSA-2009:1107
<http://www.redhat.com/support/errata/RHSA-2009-1107.html>
- * REDHAT: RHSA-2009:1108
<http://www.redhat.com/support/errata/RHSA-2009-1108.html>
- * UBUNTU: USN-786-1
<http://www.ubuntu.com/usn/usn-786-1>
- * UBUNTU: USN-787-1
<http://www.ubuntu.com/usn/usn-787-1>
- * BID: 35251
<http://www.securityfocus.com/bid/35251>
- * SECUNIA: 34724
<http://secunia.com/advisories/34724>
- * SECUNIA: 35487
<http://secunia.com/advisories/35487>
- * SECUNIA: 35395
<http://secunia.com/advisories/35395>
- * SECUNIA: 35565
<http://secunia.com/advisories/35565>
- * SECUNIA: 35710
<http://secunia.com/advisories/35710>
- * SECUNIA: 35284
<http://secunia.com/advisories/35284>
- * SECUNIA: 35843
<http://secunia.com/advisories/35843>
- * SECUNIA: 35797
<http://secunia.com/advisories/35797>
- * VUPEN: ADV-2009-1907
<http://www.vupen.com/english/advisories/2009/1907>

CVE Reference:

CVE-2009-1956 (cve.mitre.org, nvd.nist.gov)

• 18547 Apache AllowOverride Options handling bypass Vulnerability

A flaw was found in the handling of the "Options" and "AllowOverride" directives. In configurations using the "AllowOverride" directive with certain "Options=" arguments, local users were not restricted from executing commands

from a Server-Side-Include script as intended.

The issue is fixed in version 2.2.12.

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

References:

- * MLIST: [apache-httpd-dev] 20090423 Includes vs IncludesNoExec security issue - help needed
<http://marc.info/?l=apache-httpd-dev&m=124048996106302&w=2>
- * CONFIRM:
<http://svn.apache.org/viewvc?view=rev&revision=772997>
- * CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=489436
- * DEBIAN: DSA-1816
<http://www.debian.org/security/2009/dsa-1816>
- * FEDORA: FEDORA-2009-8812
<https://www.redhat.com/archives/fedora-package-announce/2009-August/msg01363.html>
- * GENTOO: GLSA-200907-04
<http://security.gentoo.org/glsa/glsa-200907-04.xml>
- * MANDRIVA: MDVSA-2009:124
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:124>
- * REDHAT: RHSA-2009:1075
<http://www.redhat.com/support/errata/RHSA-2009-1075.html>
- * REDHAT: RHSA-2009:1156
<http://www.redhat.com/support/errata/RHSA-2009-1156.html>
- * UBUNTU: USN-787-1
<http://www.ubuntu.com/usn/usn-787-1>
- * BID: 35115
<http://www.securityfocus.com/bid/35115>
- * OSVDB: 54733
<http://osvdb.org/54733>
- * SECTRACK: 1022296
<http://www.securitytracker.com/id?1022296>
- * SECUNIA: 35261
<http://secunia.com/advisories/35261>
- * SECUNIA: 35264
<http://secunia.com/advisories/35264>
- * SECUNIA: 35453
<http://secunia.com/advisories/35453>
- * SECUNIA: 35395
<http://secunia.com/advisories/35395>
- * SECUNIA: 35721
<http://secunia.com/advisories/35721>
- * VUPEN: ADV-2009-1444
<http://www.vupen.com/english/advisories/2009/1444>
- * XF: apache-allowoverrides-security-bypass(50808)
<http://xforce.iss.net/xforce/xfdb/50808>

CVE Reference:

CVE-2009-1195 (cve.mitre.org, nvd.nist.gov)

• 18548 Apache mod_deflate Denial of Service Vulnerability

A denial of service flaw was found in the mod_deflate module. This module continued to compress large files until compression was complete, even if the network connection that requested the content was closed before compression completed. This would cause mod_deflate to consume large amounts of CPU if mod_deflate was enabled for a large file.

The issue is fixed in version 2.2.12.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Attack / 100% CPU** Risk: **High**

References:

- * MLIST: [apache-httpd-dev] 20090628 mod_deflate DoS
<http://marc.info/?l=apache-httpd-dev&m=124621326524824&w=2>
- * MLIST: [apache-httpd-dev] 20090703 Re: mod_deflate DoS
<http://marc.info/?l=apache-httpd-dev&m=124661528519546&w=2>
- * MISC:
<http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=534712>

* CONFIRM:

https://bugzilla.redhat.com/show_bug.cgi?id=509125

* DEBIAN: DSA-1834

<http://www.debian.org/security/2009/dsa-1834>

* FEDORA: FEDORA-2009-8812

<https://www.redhat.com/archives/fedora-package-announce/2009-August/msg01363.html>

* GENTOO: GLSA-200907-04

<http://security.gentoo.org/glsa/glsa-200907-04.xml>

* MANDRIVA: MDVSA-2009:149

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:149>

* REDHAT: RHSA-2009:1148

<https://rhn.redhat.com/errata/RHSA-2009-1148.html>

* REDHAT: RHSA-2009:1156

<http://www.redhat.com/support/errata/RHSA-2009-1156.html>

* UBUNTU: USN-802-1

<http://www.ubuntu.com/usn/USN-802-1>

* OSVDB: 55782

<http://osvdb.org/55782>

* SECTRACK: 1022529

<http://www.securitytracker.com/id?1022529>

* SECUNIA: 35721

<http://secunia.com/advisories/35721>

* SECUNIA: 35781

<http://secunia.com/advisories/35781>

* SECUNIA: 35793

<http://secunia.com/advisories/35793>

* SECUNIA: 35865

<http://secunia.com/advisories/35865>

* VUPEN: ADV-2009-1841

<http://www.vupen.com/english/advisories/2009/1841>

* BID: 35623

<http://www.securityfocus.com/bid/35623>

CVE Reference:

CVE-2009-1891 (cve.mitre.org, nvd.nist.gov)

• 18549 Apache mod_proxy_ajp information disclosure Vulnerability

An information disclosure flaw was found in mod_proxy_ajp in version 2.2.11 only. In certain situations, if a user sent a carefully crafted HTTP request, the server could return a response intended for another user.

The issue is fixed in version 2.2.12.

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

References:

* CONFIRM:

<http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=766938&r2=767089>

* CONFIRM:

http://www.apache.org/dist/httpd/patches/apply_to_2.2.11/PR46949.diff

* CONFIRM:

https://issues.apache.org/bugzilla/show_bug.cgi?id=46949

* GENTOO: GLSA-200907-04

<http://security.gentoo.org/glsa/glsa-200907-04.xml>

* MANDRIVA: MDVSA-2009:102

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:102>

* UBUNTU: USN-787-1

<http://www.ubuntu.com/usn/usn-787-1>

* BID: 34663

<http://www.securityfocus.com/bid/34663>

* OSVDB: 53921

<http://osvdb.org/53921>

* SECTRACK: 1022264

<http://www.securitytracker.com/id?1022264>

* SECUNIA: 34827

<http://secunia.com/advisories/34827>

* SECUNIA: 35395

<http://secunia.com/advisories/35395>

* SECUNIA: 35721

<http://secunia.com/advisories/35721>

* VUPEN: ADV-2009-1147

<http://www.vupen.com/english/advisories/2009/1147>

* XF: apache-modproxyajp-information-disclosure(50059)

<http://xforce.iss.net/xforce/xfdb/50059>

CVE Reference:

CVE-2009-1191 (cve.mitre.org, nvd.nist.gov)

• 18550 Apache mod_proxy reverse proxy Denial of Service Vulnerability

A denial of service flaw was found in the mod_proxy module when it was used as a reverse proxy. A remote attacker could use this flaw to force a proxy process to consume large amounts of CPU time.

The issue is fixed in version 2.2.12.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Attack / 100% CPU** Risk: **High**

References:

* CONFIRM:

<http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?r1=790587&r2=790586&pathrev=790587>

* CONFIRM:

<http://svn.apache.org/viewvc/httpd/httpd/trunk/CHANGES?revision=790587>

* CONFIRM:

http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_http.c?r1=790587&r2=790586&pathrev=790587

* CONFIRM:

<http://svn.apache.org/viewvc?view=rev&revision=790587>

* DEBIAN: DSA-1834

<http://www.debian.org/security/2009/dsa-1834>

* FEDORA: FEDORA-2009-8812

<https://www.redhat.com/archives/fedora-package-announce/2009-August/msg01363.html>

* GENTOO: GLSA-200907-04

<http://security.gentoo.org/glsa/glsa-200907-04.xml>

* MANDRIVA: MDVSA-2009:149

<http://www.mandriva.com/security/advisories?name=MDVSA-2009:149>

* REDHAT: RHSA-2009:1148

<https://rhn.redhat.com/errata/RHSA-2009-1148.html>

* REDHAT: RHSA-2009:1156

<http://www.redhat.com/support/errata/RHSA-2009-1156.html>

* UBUNTU: USN-802-1

<http://www.ubuntu.com/usn/USN-802-1>

* BID: 35565

<http://www.securityfocus.com/bid/35565>

* OSVDB: 55553

<http://osvdb.org/55553>

* SECTRACK: 1022509

<http://www.securitytracker.com/id?1022509>

* SECUNIA: 35691

<http://secunia.com/advisories/35691>

* SECUNIA: 35721

<http://secunia.com/advisories/35721>

* SECUNIA: 35793

<http://secunia.com/advisories/35793>

* SECUNIA: 35865

<http://secunia.com/advisories/35865>

CVE Reference:

CVE-2009-1890 (cve.mitre.org, nvd.nist.gov)

• 18551 Apache APR apr_palloc heap overflow Vulnerability

A flaw in apr_palloc() in the bundled copy of APR could cause heap overflows in programs that try to apr_palloc() a user controlled size. The Apache HTTP Server itself does not pass unsanitized user-provided sizes to this function, so it could only be triggered through some other application which uses apr_palloc() in a vulnerable way.

The issue is fixed in version 2.2.13.

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

References:

* CONFIRM:
<http://svn.apache.org/viewvc/apr/apr-util/branches/0.9.x/CHANGES?revision=800736&view=markup>

* CONFIRM:
http://svn.apache.org/viewvc/apr/apr-util/branches/0.9.x/misc/apr_rmm.c?r1=230441&r2=800736

* CONFIRM:
<http://svn.apache.org/viewvc/apr/apr-util/branches/1.3.x/CHANGES?revision=800735&view=markup>

* CONFIRM:
http://svn.apache.org/viewvc/apr/apr-util/branches/1.3.x/misc/apr_rmm.c?r1=647687&r2=800735

* CONFIRM:
<http://svn.apache.org/viewvc/apr/apr/branches/0.9.x/CHANGES?revision=800733&view=markup>

* CONFIRM:
http://svn.apache.org/viewvc/apr/apr/branches/0.9.x/memory/unix/apr_pools.c?r1=585356&r2=800733

* CONFIRM:
<http://svn.apache.org/viewvc/apr/apr/branches/1.3.x/CHANGES?revision=800732&view=markup>

* CONFIRM:
http://svn.apache.org/viewvc/apr/apr/branches/1.3.x/memory/unix/apr_pools.c?r1=678140&r2=800732

* FEDORA: FEDORA-2009-8336
<https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00320.html>

* FEDORA: FEDORA-2009-8360
<https://www.redhat.com/archives/fedora-package-announce/2009-August/msg00353.html>

* MANDRIVA: MDVSA-2009:195
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:195>

* UBUNTU: USN-813-2
<http://www.ubuntu.com/usn/usn-813-2>

* BID: 35949
<http://www.securityfocus.com/bid/35949>

* OSVDB: 56765
<http://osvdb.org/56765>

* OSVDB: 56766
<http://osvdb.org/56766>

* SECUNIA: 36138
<http://secunia.com/advisories/36138>

* SECUNIA: 36140
<http://secunia.com/advisories/36140>

* SECUNIA: 36166
<http://secunia.com/advisories/36166>

* SECUNIA: 36233
<http://secunia.com/advisories/36233>

CVE Reference:

CVE-2009-2412 (cve.mitre.org, nvd.nist.gov)

• 18552 Apache mod_proxy_ftp FTP command injection Vulnerability

A flaw was found in the mod_proxy_ftp module. In a reverse proxy configuration, a remote attacker could use this flaw to bypass intended access restrictions by creating a carefully-crafted HTTP Authorization header, allowing the attacker to send arbitrary commands to the FTP server.

The issue is fixed in version 2.2.14.

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

References:

* MISC:
<http://intevydis.com/vd-list.shtml>

* BID: 36254
<http://www.securityfocus.com/bid/36254>

CVE Reference:

CVE-2009-3095 (cve.mitre.org, nvd.nist.gov)

• 18553 Apache mod_proxy_ftp Denial of Service Vulnerability

A NULL pointer dereference flaw was found in the mod_proxy_ftp module. A malicious FTP server to which requests are being proxied could use this flaw to crash an httpd child process via a malformed reply to the EPSV or PASV commands, resulting in a limited denial of service.

The issue is fixed in version 2.2.14.

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

References:

- * MISC: <http://intevydis.com/vd-list.shtml>
- * MISC: <http://www.intevydis.com/blog/?p=59>
- * SECUNIA: 36549 <http://secunia.com/advisories/36549>
- * BID: 36260 <http://www.securityfocus.com/bid/36260>

CVE Reference:

CVE-2009-3094 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2009-2679 HP CVSS 2.0 Score = 7.8

Unspecified vulnerability in bootpd in HP HP-UX B.11.11, B.11.23, and B.11.31 allows remote attackers to cause a denial of service via unknown attack vectors.

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

References:

- BID: <http://www.securityfocus.com/bid/36395>
- HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01866324>
- HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01866324>
- VUPEN: <http://www.vupen.com/english/advisories/2009/2664>
- SECUNIA: <http://secunia.com/advisories/36663>

CVE Reference: [CVE-2009-2679](#)

• CVE-2009-3570 OpenOffice CVSS 2.0 Score = 10.0

Unspecified vulnerability in OpenOffice.org (OOo) has unspecified impact and remote attack vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.9. NOTE: as of 200901005, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.

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

References:

- SECTRAK: <http://www.securitytracker.com/id?1022828>
- BID: <http://www.securityfocus.com/bid/36285>
- MISC: <http://intevydis.com/vd-list.shtml>

CVE Reference: [CVE-2009-3570](#)

• CVE-2009-3569 OpenOffice CVSS 2.0 Score = 9.3

Stack-based buffer overflow in OpenOffice.org (OOo) allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by a certain module in VulnDisco Pack Professional 8.8, aka "Client-side stack overflow exploit." NOTE: as of 20091005, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.

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

References:

- SECTRAK: <http://www.securitytracker.com/id?1022832>
- BID: <http://www.securityfocus.com/bid/36285>
- MISC: <http://intevydis.com/vd-list.shtml>

CVE Reference: [CVE-2009-3569](#)

• **CVE-2009-3571 OpenOffice CVSS 2.0 Score = 9.3**

Unspecified vulnerability in OpenOffice.org (OOo) has unknown impact and client-side attack vector, as demonstrated by a certain module in VulnDisco Pack Professional 8.8, aka "Client-side exploit." NOTE: as of 200901005, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.

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

References:

SECTRAK: <http://www.securitytracker.com/id?1022832>

BID: <http://www.securityfocus.com/bid/36285>

MISC: <http://intevydis.com/vd-list.shtml>

CVE Reference: [CVE-2009-3571](#)

• **CVE-2009-3527 FreeBSD CVSS 2.0 Score = 6.9**

Race condition in the Pipe (IPC) close function in FreeBSD 6.3 and 6.4 allows local users to cause a denial of service (crash) or gain privileges via vectors related to kqueues, which triggers a use after free, leading to a NULL pointer dereference or memory corruption.

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

References:

SECTRAK: <http://www.securitytracker.com/id?1022982>

BID: <http://www.securityfocus.com/bid/36375>

FREEBSD: <http://security.freebsd.org/advisories/FreeBSD-SA-09:13.pipe.asc>

BUGTRAQ: <http://www.securityfocus.com/archive/1/506449>

OSVDB: <http://osvdb.org/58544>

CVE Reference: [CVE-2009-3527](#)

• **CVE-2009-3572 OpenBSD CVSS 2.0 Score = 4.9**

OpenBSD 4.4, 4.5, and 4.6, when running on an i386 kernel, does not properly handle XMM exceptions, which allows local users to cause a denial of service (kernel panic) via unspecified vectors.

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

References:

BID: <http://www.securityfocus.com/bid/36589>

OPENBSD: <http://www.openbsd.org/errata46.html>

OPENBSD: <http://www.openbsd.org/errata45.html>

OPENBSD: <http://www.openbsd.org/errata44.html>

MLIST: <http://marc.info/?l=openbsd-security-announce&m=125474331811594>

SECUNIA: <http://secunia.com/advisories/36956>

CVE Reference: [CVE-2009-3572](#)

• **CVE-2009-2906 Samba CVSS 2.0 Score = 4.0**

smbd in Samba 3.0 before 3.0.37, 3.2 before 3.2.15, 3.3 before 3.3.8, and 3.4 before 3.4.2 allows remote authenticated users to cause a denial of service (infinite loop) via an unanticipated oplock break notification reply packet.

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

References:

FEDORA: <https://www.redhat.com/archives/fedora-package-announce/2009-October/msg00098.html>

FEDORA: <https://www.redhat.com/archives/fedora-package-announce/2009-October/msg00095.html>

VUPEN: <http://www.vupen.com/english/advisories/2009/2810>

UBUNTU: <http://www.ubuntu.com/usn/USN-839-1>

BID: <http://www.securityfocus.com/bid/36573>

SLACKWARE:

<http://slackware.com/security/viewer.php?l=slackware-security&y=2009&m=slackware-security.561439>

XF: <http://xforce.iss.net/xforce/xfdb/53575>

SECTRAK: <http://www.securitytracker.com/id?1022976>

SECUNIA: <http://secunia.com/advisories/36953>

SECUNIA: <http://secunia.com/advisories/36937>

SECUNIA: <http://secunia.com/advisories/36918>

SECUNIA: <http://secunia.com/advisories/36893>

CONFIRM: <http://samba.org/samba/security/CVE-2009-2906.html>

OSVDB: <http://osvdb.org/58519>

CVE Reference: [CVE-2009-2906](#)

• **CVE-2009-2948 Samba CVSS 2.0 Score = 1.9**

mount.cifs in Samba 3.0 before 3.0.37, 3.2 before 3.2.15, 3.3 before 3.3.8 and 3.4 before 3.4.2, when mount.cifs is installed suid root, does not properly enforce permissions, which allows local users to read part of the credentials file and obtain the password by specifying the path to the credentials file and using the --verbose or -v option.

Test Case Impact: Vulnerability Impact: Risk: **Low**

References:

FEDORA: <https://www.redhat.com/archives/fedora-package-announce/2009-October/msg00098.html>

FEDORA: <https://www.redhat.com/archives/fedora-package-announce/2009-October/msg00095.html>

UBUNTU: <http://www.ubuntu.com/usn/USN-839-1>

SECTRAK: <http://www.securitytracker.com/id?1022975>

BID: <http://www.securityfocus.com/bid/36572>

CONFIRM: <http://www.samba.org/samba/security/CVE-2009-2948.html>

SLACKWARE:

<http://slackware.com/security/viewer.php?l=slackware-security&y=2009&m=slackware-security.561439>

XF: <http://xforce.iss.net/xforce/xfdb/53574>

VUPEN: <http://www.vupen.com/english/advisories/2009/2810>

SECUNIA: <http://secunia.com/advisories/36953>

SECUNIA: <http://secunia.com/advisories/36937>

SECUNIA: <http://secunia.com/advisories/36918>

SECUNIA: <http://secunia.com/advisories/36893>

OSVDB: <http://osvdb.org/58520>

CVE Reference: [CVE-2009-2948](#)

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