

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

Tabnabbing: A new phishing technique. Credit card company fails to encrypt data. Google's wi-fi mishap ends with suit. Corporate PCs littered with malware.

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

• New phishing technique exploits browser tab use

A leading Firefox developer has discovered a new phishing attack method.

The attack, dubbed "tabnabbing," preys on browser tabs and the fact that users generally don't keep track of all the tabs they have open at one time, said Aza Raskin, creative lead for Mozilla's Firefox web browser, who discovered and publicized the technique.

In this type of phish, a user must be tricked into visiting a maliciously crafted tabbed page containing JavaScript, Raskin said. This allows the attacker to surreptitiously change the contents of a separately tabbed page, in addition to the name and logo on that tab. SC Magazine

Full Story :

http://www.scmagazineus.com/new-phishing-technique-exploits-browser-tab-use/article/170983/?utm_source=feedb

• American Express may have failed to encrypt data

American Express may be in hot water after a computer engineer discovered a portion of the card brand's website, which claims to be secure, is sending private information in the clear.

Joe Damato wrote in a blog post Tuesday that he received a promotional email from American Express encouraging him to sign up for the Daily Wish service, through which cardholders can receive hefty discounts on a limited amount of merchandise, such as computers and camcorders.

If users click on the "Sign up for Daily Wish" button, they are prompted to enter personal information, such as name, card number, security code, expiration date and billing zip code, into a pop-up box. The box includes a "This page is secure" notification link, but upon further review, Damato found this not to be the case. SC Magazine

Full Story :

http://www.scmagazineus.com/american-express-may-have-failed-to-encrypt-data/article/170997/?utm_source=feedburner&utm_medium=email&utm_campaign=american-express-may-have-failed-to-encrypt-data

• Google sued for data collection via Wi-Fi

Google this week was hit with a third class-action lawsuit over its admitted collection of information from unprotected Wi-Fi networks. The most recent lawsuit was filed on Tuesday in a federal district court in Massachusetts by Carp Law Offices on behalf of internet service provider Galaxy Internet Services and its wireless customers, along with all other affected Wi-Fi users in Massachusetts. According to the complaint, Google's collection of "payload" data - the information sent to and from users over Wi-Fi networks - was in violation of Massachusetts' new data privacy law, as well as federal regulations.

Galaxy Internet Services is seeking damages totaling \$10 million on behalf of itself and its customers. In addition, Google is facing two similar lawsuits over the privacy violation filed last week in Oregon and California. SC Magazine

Full Story :

http://www.scmagazineus.com/google-sued-for-data-collection-via-wi-fi/article/171089/?utm_source=feedburner&utm_medium=email&utm_campaign=google-sued-for-data-collection-via-wi-fi

• Survey: Corporate PCs cluttered with malware

Despite the efforts of IT departments, many PCs in the corporate and government world are littered with unauthorized software, most notably malware, says application-whitelisting company Bit9.

The results of Bit9's "2010 What's Running on Your Users' Desktops?" survey, released Monday, uncovered PCs with a significant amount of non-business software, including games, toolbars, and torrent software. Of greater concern, IT pros surveyed also discovered malware, such as ransom-ware, Trojans, and Chinese spyware.

Among the 1,282 IT professionals questioned for the survey, 68 percent of them said they have software restrictions in place, but 45 percent said they still found unauthorized software on more than half of their client PCs. Cnet Security

Full Story :

http://news.cnet.com/8301-1009_3-20006013-83.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 12167 PostgreSQL missing privilege checks for "ALTER USER" and "ALTER DATABASE" statements Vulnerability

PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, and 8.4 before 8.4.4 does not properly check privileges during certain RESET ALL operations, which allows remote authenticated users to remove arbitrary parameter settings via a ALTER USER or ALTER DATABASE statement.

PostgreSQL versions prior to 7.4.29, 8.0.25, 8.1.21, 8.2.17, 8.3.11, or 8.4.4 are vulnerable to this issue.

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

References:

- * CONFIRM:
<http://www.postgresql.org/docs/current/static/release-7-4-29.html>
- * CONFIRM:
<http://www.postgresql.org/docs/current/static/release-8-0-25.html>
- * CONFIRM:
<http://www.postgresql.org/docs/current/static/release-8-1-21.html>
- * CONFIRM:
<http://www.postgresql.org/docs/current/static/release-8-2-17.html>
- * CONFIRM:
<http://www.postgresql.org/docs/current/static/release-8-3-11.html>
- * CONFIRM:

<http://www.postgresql.org/docs/current/static/release-8-4-4.html>

* MANDRIVA: MDVSA-2010:103

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:103>

* BID: 40304

<http://www.securityfocus.com/bid/40304>

* VUPEN: ADV-2010-1207

<http://www.vupen.com/english/advisories/2010/1207>

CVE Reference:

CVE-2010-1975 (cve.mitre.org, nvd.nist.gov)

• 12168 PostgreSQL error in PL/Perl related to Safe.pm arbitrary Perl code execution Vulnerability (CVE-2010-1447)

PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, 8.4 before 8.4.4, and 9.0 Beta before 9.0 Beta 2 does not properly restrict PL/perl procedures, which might allow remote attackers to execute arbitrary Perl code via a crafted script, related to the Safe module (aka Safe.pm) for Perl.

PostgreSQL versions prior to 7.4.29, 8.0.25, 8.1.21, 8.2.17, 8.3.11, or 8.4.4 are vulnerable to this issue.

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

References:

* CONFIRM:

<http://security-tracker.debian.org/tracker/CVE-2010-1447>

* CONFIRM:

<http://www.postgresql.org/about/news.1203>

* CONFIRM:

<https://bugs.launchpad.net/bugs/cve/2010-1447>

* CONFIRM:

https://bugzilla.redhat.com/show_bug.cgi?id=588269

* OSVDB: 64756

<http://osvdb.org/64756>

* SECTRACK: 1023988

<http://www.securitytracker.com/id?1023988>

* SECUNIA: 39845

<http://secunia.com/advisories/39845>

* VUPEN: ADV-2010-1167

<http://www.vupen.com/english/advisories/2010/1167>

CVE Reference:

CVE-2010-1447 (cve.mitre.org, nvd.nist.gov)

• 12169 PostgreSQL Insecure permissions on the "pltcl_modules" arbitrary Tcl code execution Vulnerability

The PL/Tcl implementation in PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, 8.4 before 8.4.4, and 9.0 Beta before 9.0 Beta 2 loads Tcl code from the pltcl_modules table regardless of the table's ownership and permissions, which allows remote authenticated users, with database-creation privileges, to execute arbitrary Tcl code by creating this table and inserting a crafted Tcl script.

PostgreSQL versions prior to 7.4.29, 8.0.25, 8.1.21, 8.2.17, 8.3.11, or 8.4.4 are vulnerable to this issue.

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

References:

* CONFIRM:

<http://www.postgresql.org/about/news.1203>

* CONFIRM:

<http://www.postgresql.org/docs/current/static/release-7-4-29.html>

* CONFIRM:

<http://www.postgresql.org/docs/current/static/release-8-0-25.html>

* CONFIRM:

<http://www.postgresql.org/docs/current/static/release-8-1-21.html>

* CONFIRM:

<http://www.postgresql.org/docs/current/static/release-8-2-17.html>

* CONFIRM:

<http://www.postgresql.org/docs/current/static/release-8-3-11.html>

* CONFIRM:

<http://www.postgresql.org/docs/current/static/release-8-4-4.html>

* CONFIRM:

<http://www.postgresql.org/support/security>

* CONFIRM:

https://bugzilla.redhat.com/show_bug.cgi?id=583072

* MANDRIVA: MDVSA-2010:103

<http://www.mandriva.com/security/advisories?name=MDVSA-2010:103>

* REDHAT: RHSA-2010:0427

<http://www.redhat.com/support/errata/RHSA-2010-0427.html>

* REDHAT: RHSA-2010:0428

<http://www.redhat.com/support/errata/RHSA-2010-0428.html>

* REDHAT: RHSA-2010:0429

<http://www.redhat.com/support/errata/RHSA-2010-0429.html>

* REDHAT: RHSA-2010:0430

<http://www.redhat.com/support/errata/RHSA-2010-0430.html>

* BID: 40215

<http://www.securityfocus.com/bid/40215>

* OSVDB: 64757

<http://osvdb.org/64757>

* SECTrack: 1023987

<http://www.securitytracker.com/id?1023987>

* SECUNIA: 39845

<http://secunia.com/advisories/39845>

* SECUNIA: 39820

<http://secunia.com/advisories/39820>

* SECUNIA: 39898

<http://secunia.com/advisories/39898>

* VUPEN: ADV-2010-1167

<http://www.vupen.com/english/advisories/2010/1167>

* VUPEN: ADV-2010-1207

<http://www.vupen.com/english/advisories/2010/1207>

* VUPEN: ADV-2010-1197

<http://www.vupen.com/english/advisories/2010/1197>

* VUPEN: ADV-2010-1198

<http://www.vupen.com/english/advisories/2010/1198>

CVE Reference:

CVE-2010-1170 (cve.mitre.org, nvd.nist.gov)

• 12170 PostgreSQL error in PL/Perl related to Safe.pm arbitrary Perl code execution Vulnerability (CVE-2010-1169)

PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, 8.4 before 8.4.4, and 9.0 Beta before 9.0 Beta 2 does not properly restrict PL/perl procedures, which might allow remote attackers to execute arbitrary Perl code via a crafted script, related to the Safe module (aka Safe.pm) for Perl.

PostgreSQL versions prior to 7.4.29, 8.0.25, 8.1.21, 8.2.17, 8.3.11, or 8.4.4 are vulnerable to this issue.

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

References:

* CONFIRM:

<http://www.postgresql.org/about/news.1203>

* CONFIRM:

<http://www.postgresql.org/docs/current/static/release-7-4-29.html>

* CONFIRM:

<http://www.postgresql.org/docs/current/static/release-8-0-25.html>

* CONFIRM:

<http://www.postgresql.org/docs/current/static/release-8-1-21.html>

* CONFIRM:

<http://www.postgresql.org/docs/current/static/release-8-2-17.html>

* CONFIRM:

<http://www.postgresql.org/docs/current/static/release-8-3-11.html>

* CONFIRM:

<http://www.postgresql.org/docs/current/static/release-8-4-4.html>

* CONFIRM:

<http://www.postgresql.org/support/security>

* CONFIRM:

https://bugzilla.redhat.com/show_bug.cgi?id=582615

* MANDRIVA: MDVSA-2010:103
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:103>
* REDHAT: RHSA-2010:0427
<http://www.redhat.com/support/errata/RHSA-2010-0427.html>
* REDHAT: RHSA-2010:0428
<http://www.redhat.com/support/errata/RHSA-2010-0428.html>
* REDHAT: RHSA-2010:0429
<http://www.redhat.com/support/errata/RHSA-2010-0429.html>
* REDHAT: RHSA-2010:0430
<http://www.redhat.com/support/errata/RHSA-2010-0430.html>
* BID: 40215
<http://www.securityfocus.com/bid/40215>
* OSVDB: 64755
<http://osvdb.org/64755>
* SECTRAK: 1023988
<http://www.securitytracker.com/id?1023988>
* SECUNIA: 39845
<http://secunia.com/advisories/39845>
* SECUNIA: 39820
<http://secunia.com/advisories/39820>
* SECUNIA: 39898
<http://secunia.com/advisories/39898>
* VUPEN: ADV-2010-1167
<http://www.vupen.com/english/advisories/2010/1167>
* VUPEN: ADV-2010-1207
<http://www.vupen.com/english/advisories/2010/1207>
* VUPEN: ADV-2010-1197
<http://www.vupen.com/english/advisories/2010/1197>
* VUPEN: ADV-2010-1198
<http://www.vupen.com/english/advisories/2010/1198>
* XF: postgresql-safe-code-execution(58693)
<http://xforce.iss.net/xforce/xfdb/58693>

CVE Reference:

CVE-2010-1169 (cve.mitre.org, nvd.nist.gov)

• 12171 PostgreSQL Integer overflow in nodeHash.c Vulnerability

Integer overflow in src/backend/executor/nodeHash.c in PostgreSQL 8.4.1 and earlier, and 8.5 through 8.5alpha2, allows remote authenticated users to cause a denial of service (daemon crash) via a SELECT statement with many LEFT JOIN clauses, related to certain hashtable size calculations.

PostgreSQL versions prior to 8.4.2 are vulnerable to this issue.

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

References:

* MLIST: [oss-security] 20100309 CVE Request: postgresql integer overflow in hash table size calculation
<http://www.openwall.com/lists/oss-security/2010/03/09/2>
* MLIST: [oss-security] 20100316 Re: CVE Request: postgresql integer overflow in hash table size calculation
<http://www.openwall.com/lists/oss-security/2010/03/16/10>
* MLIST: [pgsql-bugs] 20091028 BUG #5145: Complex query with lots of LEFT JOIN causes segfault
<http://archives.postgresql.org/pgsql-bugs/2009-10/msg00277.php>
* MLIST: [pgsql-bugs] 20091029 Re: BUG #5145: Complex query with lots of LEFT JOIN causes segfault
<http://archives.postgresql.org/pgsql-bugs/2009-10/msg00287.php>
* MLIST: [pgsql-bugs] 20091029 Re: BUG #5145: Complex query with lots of LEFT JOIN causes segfault
<http://archives.postgresql.org/pgsql-bugs/2009-10/msg00289.php>
* MLIST: [pgsql-bugs] 20091030 Re: BUG #5145: Complex query with lots of LEFT JOIN causes segfault
<http://archives.postgresql.org/pgsql-bugs/2009-10/msg00310.php>
* CONFIRM:
<http://git.postgresql.org/gitweb?p=postgresql.git;a=commit;h=64b057e6823655fb6c5d1f24a28f236b94dd6c54>
* CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=546621
* REDHAT: RHSA-2010:0427
<http://www.redhat.com/support/errata/RHSA-2010-0427.html>
* REDHAT: RHSA-2010:0428
<http://www.redhat.com/support/errata/RHSA-2010-0428.html>
* REDHAT: RHSA-2010:0429
<http://www.redhat.com/support/errata/RHSA-2010-0429.html>

* BID: 38619
<http://www.securityfocus.com/bid/38619>
* SECUNIA: 39820
<http://secunia.com/advisories/39820>
* VUPEN: ADV-2010-1197
<http://www.vupen.com/english/advisories/2010/1197>

CVE Reference:

CVE-2010-0733 (cve.mitre.org, nvd.nist.gov)

• 12172 PostgreSQL bitsubstr function Denial of Service Vulnerability

The bitsubstr function in backend/utils/adt/varbit.c in PostgreSQL 8.0.23, 8.1.11, and 8.3.8 allows remote authenticated users to cause a denial of service (daemon crash) or have unspecified other impact via vectors involving a negative integer in the third argument, as demonstrated by a SELECT statement that contains a call to the substring function for a bit string, related to an "overflow."

PostgreSQL versions prior to 8.0.24, 8.1.12, and 8.3.9 are vulnerable to this issue.

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

References:

* MLIST: [oss-security] 20100127 Re: CVE id request: postgresql bitsubstr overflow
<http://www.openwall.com/lists/oss-security/2010/01/27/5>
* MLIST: [pgsql-committers] 20100107 pgsq: Make bit/varbit substring() treat any negative length as meaning
<http://archives.postgresql.org/pgsql-committers/2010-01/msg00125.php>
* MLIST: [pgsql-hackers] 20100107 Re: Patch: Allow substring/replace() to get/set bit values
<http://archives.postgresql.org/pgsql-hackers/2010-01/msg00634.php>
* MISC:
<http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=567058>
* MISC:
<http://intevydis.blogspot.com/2010/01/postgresql-8023-bitsubstr-overflow.html>
* CONFIRM:
<http://git.postgresql.org/gitweb?p=postgresql.git;a=commit;h=75dea10196c31d98d98c0bafceb576ae99c09b12>
* CONFIRM:
<http://git.postgresql.org/gitweb?p=postgresql.git;a=commit;h=b15087cb39ca9e4bde3c8920fcee3741045d2b83>
* CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=559194
* CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=559259
* MANDRIVA: MDVSA-2010:103
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:103>
* REDHAT: RHSA-2010:0427
<http://www.redhat.com/support/errata/RHSA-2010-0427.html>
* REDHAT: RHSA-2010:0428
<http://www.redhat.com/support/errata/RHSA-2010-0428.html>
* REDHAT: RHSA-2010:0429
<http://www.redhat.com/support/errata/RHSA-2010-0429.html>
* UBUNTU: USN-933-1
<http://ubuntu.com/usn/usn-933-1>
* BID: 37973
<http://www.securityfocus.com/bid/37973>
* SECTRAK: 1023510
<http://securitytracker.com/id?1023510>
* SECUNIA: 39566
<http://secunia.com/advisories/39566>
* SECUNIA: 39820
<http://secunia.com/advisories/39820>
* VUPEN: ADV-2010-1022
<http://www.vupen.com/english/advisories/2010/1022>
* VUPEN: ADV-2010-1207
<http://www.vupen.com/english/advisories/2010/1207>
* VUPEN: ADV-2010-1197
<http://www.vupen.com/english/advisories/2010/1197>
* XF: postgresql-substring-bo(55902)
<http://xforce.iss.net/xforce/xfdb/55902>

CVE Reference:

CVE-2010-0442 (cve.mitre.org, nvd.nist.gov)

• 12173 PostgreSQL session-local state privileges escalation Vulnerability

PostgreSQL 7.4.x before 7.4.27, 8.0.x before 8.0.23, 8.1.x before 8.1.19, 8.2.x before 8.2.15, 8.3.x before 8.3.9, and 8.4.x before 8.4.2 does not properly manage session-local state during execution of an index function by a database superuser, which allows remote authenticated users to gain privileges via a table with crafted index functions, as demonstrated by functions that modify (1) search_path or (2) a prepared statement, a related issue to CVE-2007-6600 and CVE-2009-3230.

PostgreSQL versions prior to 7.4.27, 8.0.23, 8.1.19, 8.2.15, 8.3.9, 8.4.2 are vulnerable to this issue.

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

References:

- * BUGTRAQ: 20100307 rPSA-2010-0012-1 postgresql postgresql-contrib postgresql-server
<http://www.securityfocus.com/archive/1/archive/1/509917/100/0/threaded>
- * CONFIRM:
<http://www.postgresql.org/docs/current/static/release-7-4-27.html>
- * CONFIRM:
<http://www.postgresql.org/docs/current/static/release-8-0-23.html>
- * CONFIRM:
<http://www.postgresql.org/docs/current/static/release-8-1-19.html>
- * CONFIRM:
<http://www.postgresql.org/docs/current/static/release-8-2-15.html>
- * CONFIRM:
<http://www.postgresql.org/docs/current/static/release-8-3-9.html>
- * CONFIRM:
<http://www.postgresql.org/docs/current/static/release-8-4-2.html>
- * CONFIRM:
<http://www.postgresql.org/support/security.html>
- * CONFIRM:
https://bugzilla.redhat.com/show_bug.cgi?id=546321
- * CONFIRM:
<http://wiki.rpath.com/wiki/Advisories:rPSA-2010-0012>
- * FEDORA: FEDORA-2009-13363
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg01035.html>
- * FEDORA: FEDORA-2009-13381
<https://www.redhat.com/archives/fedora-package-announce/2009-December/msg01056.html>
- * MANDRIVA: MDVSA-2009:333
<http://www.mandriva.com/security/advisories?name=MDVSA-2009:333>
- * REDHAT: RHSA-2010:0427
<http://www.redhat.com/support/errata/RHSA-2010-0427.html>
- * REDHAT: RHSA-2010:0428
<http://www.redhat.com/support/errata/RHSA-2010-0428.html>
- * REDHAT: RHSA-2010:0429
<http://www.redhat.com/support/errata/RHSA-2010-0429.html>
- * SUSE: SUSE-SR:2010:001
<http://lists.opensuse.org/opensuse-security-announce/2010-01/msg00007.html>
- * BID: 37333
<http://www.securityfocus.com/bid/37333>
- * OSVDB: 61039
<http://osvdb.org/61039>
- * SECTRAK: 1023326
<http://www.securitytracker.com/id?1023326>
- * SECUNIA: 37663
<http://secunia.com/advisories/37663>
- * SECUNIA: 39820
<http://secunia.com/advisories/39820>
- * VUPEN: ADV-2009-3519
<http://www.vupen.com/english/advisories/2009/3519>
- * VUPEN: ADV-2010-1197
<http://www.vupen.com/english/advisories/2010/1197>

CVE Reference:

CVE-2009-4136 (cve.mitre.org, nvd.nist.gov)

• 14351 RealVNC Remote Authentication Bypass Vulnerability

RealVNC 4.1.1, and other products that use RealVNC such as AdderLink IP and Cisco CallManager, allows remote attackers to bypass authentication via a request in which the client specifies an insecure security type such as "Type 1 - None", which is accepted even if it is not offered by the server.

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

References:

- * BUGTRAQ: 20060516 re: RealVNC 4.1.1 Remote Compromise
<http://www.securityfocus.com/archive/1/archive/1/434117/100/0/threaded>
- * BUGTRAQ: 20060518 RE: [Full-disclosure] RealVNC 4.1.1 Remote Compromise
<http://www.securityfocus.com/archive/1/archive/1/434518/100/0/threaded>
- * BUGTRAQ: 20060520 Re: [Full-disclosure] RealVNC 4.1.1 Remote Compromise
<http://www.securityfocus.com/archive/1/archive/1/434560/100/0/threaded>
- * BUGTRAQ: 20060623 Linux VNC evil client patch - BID 17978
<http://www.securityfocus.com/archive/1/archive/1/438175/100/0/threaded>
- * BUGTRAQ: 20060624 Re: Linux VNC evil client patch - BID 17978
<http://www.securityfocus.com/archive/1/archive/1/438368/100/0/threaded>
- * MISC:
<http://www.intelliadmin.com/blog/2006/05/security-flaw-in-realvnc-411.html>
- * MISC:
<http://www.intelliadmin.com/blog/2006/05/vnc-flaw-proof-of-concept.html>
- * FULLDISC: 20060515 RealVNC 4.1.1 Remote Compromise
<http://marc.theaimsgroup.com/?l=full-disclosure&m=11476834411131&w=2>
- * BUGTRAQ: 20060515 RealVNC 4.1.1 Remote Compromise
<http://www.securityfocus.com/archive/1/archive/1/433994/100/0/threaded>
- * BUGTRAQ: 20060515 Re: [Full-disclosure] RealVNC 4.1.1 Remote Compromise
<http://www.securityfocus.com/archive/1/archive/1/434015/100/0/threaded>
- * MLIST: [vnc-list] 20060513 Version 4.1.2
<http://marc.theaimsgroup.com/?l=vnc-list&m=114755444130188&w=2>
- * CONFIRM:
<http://www.realvnc.com/products/free/4.1/release-notes.html>
- * CISCO: 20060622 RealVNC Remote Authentication Bypass Vulnerability
<http://www.cisco.com/warp/public/707/cisco-sr-20060622-cmm.shtml>
- * CERT-VN: VU#117929
<http://www.kb.cert.org/vuls/id/117929>
- * BID: 17978
<http://www.securityfocus.com/bid/17978>
- * VUPEN: ADV-2006-1821
<http://www.vupen.com/english/advisories/2006/1821>
- * VUPEN: ADV-2006-1790
<http://www.vupen.com/english/advisories/2006/1790>
- * VUPEN: ADV-2006-2492
<http://www.vupen.com/english/advisories/2006/2492>
- * OSVDB: 25479
<http://www.osvdb.org/25479>
- * SECTRAK: 1016083
<http://securitytracker.com/id?1016083>
- * SECUNIA: 20107
<http://secunia.com/advisories/20107>
- * SECUNIA: 20109
<http://secunia.com/advisories/20109>
- * SECUNIA: 20789
<http://secunia.com/advisories/20789>
- * XF: realvnc-auth-bypass(26445)
<http://xforce.iss.net/xforce/xfdb/26445>

CVE Reference:

CVE-2006-2369 (cve.mitre.org, nvd.nist.gov)

• 18813 Outlook Express and Windows Mail Integer Overflow Vulnerability (MS10-030/978542) (Remote File Checking)

An unauthenticated remote code execution vulnerability exists in the way that Windows Mail Client handles specially crafted mail responses. An attempt to exploit the vulnerability would not require authentication, allowing an attacker to exploit the vulnerability by sending a specially crafted response to a client initiating a connection to a server under his control using the common mail protocols POP3 and IMAP.

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

References:

- * BUGTRAQ: 20100511 {PRL} Microsoft Windows Outlook Express and Windows Mail Integer Overflow
<http://archives.neohapsis.com/archives/bugtraq/2010-05/0068.html>

* MISC:

http://www.protekresearchlab.com/index.php?option=com_content&view=article&id=13&Itemid=13

* MS: MS10-030

<http://www.microsoft.com/technet/security/Bulletin/MS10-030.mspx>

* BID: 40052

<http://www.securityfocus.com/bid/40052>

* VUPEN: VUPEN/ADV-2010-1111

<http://www.vupen.com/english/advisories/2010/1111>

* SECTRAK: 1023972

<http://securitytracker.com/alerts/2010/May/1023972.html>

CVE Reference:

CVE-2010-0816 (cve.mitre.org, nvd.nist.gov)

• 18814 VBE6.dll Stack Memory Corruption Vulnerability (MS10-031/978213) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Visual Basic for Applications searches for ActiveX controls. This vulnerability could allow remote code execution if a host application opens and passes a specially crafted file to the Visual Basic for Applications runtime. 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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

References:

* MS: MS10-031

<http://www.microsoft.com/technet/security/Bulletin/MS10-031.mspx>

* VUPEN: VUPEN/ADV-2010-1121

<http://www.vupen.com/english/advisories/2010/1121>

* SECTRAK: 1023974

<http://securitytracker.com/alerts/2010/May/1023974.html>

* CONFIRM: MS10-031: VBE6 Single-Byte Stack Overwrite

<http://blogs.technet.com/srd/archive/2010/05/11/ms10-031-vbe6-single-byte-stack-overwrite.aspx>

* BID: 39931

<http://www.securityfocus.com/bid/39931>

CVE Reference:

CVE-2010-0815 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2010-2083 Microsoft CVSS 2.0 Score = 4.0

Microsoft Dynamics GP has a default value of ACCESS for the system password, which might make it easier for remote authenticated users to bypass intended access restrictions via unspecified vectors.

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

References:

MISC: <http://www.christopherkois.com/?p=448>

CVE Reference: [CVE-2010-2083](http://cve.mitre.org/cve/2010/2083)

• CVE-2010-2025 Cisco CVSS 2.0 Score = 6.8

Multiple cross-site request forgery (CSRF) vulnerabilities in the web interface on the Cisco Scientific Atlanta WebSTAR DPC2100R2 cable modem with firmware 2.0.2r1256-060303 allow remote attackers to hijack the authentication of administrators for requests that (1) reset the modem, (2) erase the firmware, (3) change the administrative password, (4) install modified firmware, or (5) change the access level, as demonstrated by a request to goform/_asvl.

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

References:

BID: <http://www.securityfocus.com/bid/40346>

FULLDISC: <http://archives.neohapsis.com/archives/fulldisclosure/2010-05/0322.html>

CVE Reference: [CVE-2010-2025](#)

• **CVE-2010-2026 Cisco CVSS 2.0 Score = 6.4**

The web interface on the Cisco Scientific Atlanta WebSTAR DPC2100R2 cable modem with firmware 2.0.2r1256-060303 allows remote attackers to bypass authentication, and reset the modem or replace the firmware, via a direct request to an unspecified page.

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

References:

BID: <http://www.securityfocus.com/bid/40346>

FULLDISC: <http://archives.neohapsis.com/archives/fulldisclosure/2010-05/0322.html>

CVE Reference: [CVE-2010-2026](#)

• **CVE-2010-2082 Cisco CVSS 2.0 Score = 5.0**

The web interface on the Cisco Scientific Atlanta WebSTAR DPC2100R2 cable modem with firmware 2.0.2r1256-060303 has a default administrative password (aka SAPassword) of W2402, which makes it easier for remote attackers to obtain privileged access.

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

References:

FULLDISC: <http://archives.neohapsis.com/archives/fulldisclosure/2010-05/0322.html>

CVE Reference: [CVE-2010-2082](#)

• **CVE-2009-4878 Novell CVSS 2.0 Score = 4.3**

Unspecified vulnerability in the Administration Console in Novell Access Manager before 3.1 SP1 allows attackers to access system files via unknown attack vectors.

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

References:

XF: <http://xforce.iss.net/xforce/xfdb/51822>

VUPEN: <http://www.vupen.com/english/advisories/2009/1945>

SECTRAK: <http://www.securitytracker.com/id?1022581>

BID: <http://www.securityfocus.com/bid/35734>

CONFIRM:

http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.htm

SECUNIA: <http://secunia.com/advisories/35898>

CVE Reference: [CVE-2009-4878](#)

• **CVE-2009-4879 Novell CVSS 2.0 Score = 4.3**

The Identity Server in Novell Access Manager before 3.1 SP1 allows attackers with disabled Active Directory accounts to authenticate using X.509 authentication, which bypasses intended access restrictions.

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

References:

SECTRAK: <http://www.securitytracker.com/id?1022581>

CONFIRM:

http://www.novell.com/documentation/novellaccessmanager31/accessmanager_readme/data/accessmanager_readme.htm

CVE Reference: [CVE-2009-4879](#)

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