

[SECURITY] [DSA 1530-1] New cupsys packages fix multiple vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-03/msg00327.html>

- *From:* Noah Meyerhans <noahm@xxxxxxxxxx>
 - *Date:* Tue, 25 Mar 2008 16:10:49 +0100
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Debian Security Advisory DSA-1530-1 security@xxxxxxxxxx
<http://www.debian.org/security/> Noah Meyerhans
March 25, 2008 <http://www.debian.org/security/faq>

Package : cupsys
Vulnerability : multiple
Problem type : remote
Debian-specific: no
CVE Id(s) : CVE-2008-0047 CVE-2008-0882
Debian Bug : 472105 467653

Several local/remote vulnerabilities have been discovered in cupsys, the Common Unix Printing System. The Common Vulnerabilities and Exposures project identifies the following problems:

CVE-2008-0047

Heap-based buffer overflow in CUPS, when printer sharing is enabled, allows remote attackers to execute arbitrary code via crafted search expressions.

CVE-2008-0882

Double free vulnerability in the `process_browse_data` function in CUPS 1.3.5 allows remote attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via crafted packets to the cupsd port (631/udp), related to an unspecified manipulation of a remote printer.

For the stable distribution (etch), these problems have been fixed in version 1.2.7-4etch3

We recommend that you upgrade your cupsys packages.

Upgrade instructions

[SECURITY] [DSA 1530-1] New cupsys packages fix multiple vulnerabilities

wget url
will fetch the file for you
dpkg -i file.deb
will install the referenced file.

If you are using the apt-get package manager, use the line for sources.list as given below:

apt-get update
will update the internal database
apt-get upgrade
will install corrected packages

You may use an automated update by adding the resources from the footer to the proper configuration.

Debian GNU/Linux 4.0 alias etch

Stable updates are available for alpha, amd64, i386, ia64, mips, mipsel, powerpc, s390 and sparc.

Source archives:

http://security.debian.org/pool/updates/main/c/cupsys/cupsys_1.2.7-4etch3.diff.gz
Size/MD5 checksum: 104776 b684811e24921a7574798108ac6988d7
http://security.debian.org/pool/updates/main/c/cupsys/cupsys_1.2.7-4etch3.dsc
Size/MD5 checksum: 1084 0276f8e59e00181d39d204a28494d18c
http://security.debian.org/pool/updates/main/c/cupsys/cupsys_1.2.7.orig.tar.gz
Size/MD5 checksum: 4214272 c9ba33356e5bb93efbcf77b6e142e498

Architecture independent packages:

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-common_1.2.7-4etch3_all.deb
Size/MD5 checksum: 927322 65b1ff3cb7b8bbbe3b334ee43875aac4
http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2-gnutls10_1.2.7-4etch3_all.deb
Size/MD5 checksum: 45654 0b4ce3e9c2af460c5b694b906f450b12

alpha architecture (DEC Alpha)

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-dbg_1.2.7-4etch3_alpha.deb
Size/MD5 checksum: 1097006 45800a6b2c1dd7068843ade84480259d
http://security.debian.org/pool/updates/main/c/cupsys/cupsys-bsd_1.2.7-4etch3_alpha.deb
Size/MD5 checksum: 39262 4f645e439999611b07348ad50e4da57d
http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2_1.2.7-4etch3_alpha.deb
Size/MD5 checksum: 174890 9affa7a1f2dc6548fcffb9a456181a3a
http://security.debian.org/pool/updates/main/c/cupsys/cupsys-client_1.2.7-4etch3_alpha.deb
Size/MD5 checksum: 86292 23431d4bfae9599caba759d4b0a3a8c0
http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2_1.2.7-4etch3_alpha.deb
Size/MD5 checksum: 94814 6be946280a3c9fadfd070f7284255df0

[SECURITY] [DSA 1530-1] New cupsys packages fix multiple vulnerabilities

http://security.debian.org/pool/updates/main/c/cupsys/cupsys_1.2.7-4etch3_alpha.deb

Size/MD5 checksum: 1609104 ecdd9f65f8799605a1efeac0d4eae774

http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2-dev_1.2.7-4etch3_alpha.deb

Size/MD5 checksum: 184372 7720c886672d63cdeb501314beacc4b5

http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2-dev_1.2.7-4etch3_alpha.deb

Size/MD5 checksum: 72428 2b4ed65a0a33b7cf32756c2b0cd925de

amd64 architecture (AMD x86_64 (AMD64))

http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2-dev_1.2.7-4etch3_amd64.deb

Size/MD5 checksum: 52858 badd0d21043714aa2c612b45323890a1

http://security.debian.org/pool/updates/main/c/cupsys/cupsys_1.2.7-4etch3_amd64.deb

Size/MD5 checksum: 1574654 cf1c04e898f7380fdd338ecafb69185e

http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2_1.2.7-4etch3_amd64.deb

Size/MD5 checksum: 85652 24c3d3e054306785ccc958f1894a2b18

http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2-dev_1.2.7-4etch3_amd64.deb

Size/MD5 checksum: 142534 7ad95206e0e450f8df27c9d858809ddb

http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2_1.2.7-4etch3_amd64.deb

Size/MD5 checksum: 162008 44f8d076b07194023c8ef4348a56e97a

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-bsd_1.2.7-4etch3_amd64.deb

Size/MD5 checksum: 36352 5a4f9dc02fa0f8fb6936859c0fb1bd61

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-dbg_1.2.7-4etch3_amd64.deb

Size/MD5 checksum: 1086740 d466f2f5d8cb17ae0013dd99db5bcb0

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-client_1.2.7-4etch3_amd64.deb

Size/MD5 checksum: 80704 d45a4a7461defd4c6b96bbfc292e3183

i386 architecture (Intel ia32)

http://security.debian.org/pool/updates/main/c/cupsys/cupsys_1.2.7-4etch3_i386.deb

Size/MD5 checksum: 1565044 7c19a56cb4a782487e104a01f31e0b47

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-bsd_1.2.7-4etch3_i386.deb

Size/MD5 checksum: 37600 fa90419b34b6733ef32f13797e4606f3

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-client_1.2.7-4etch3_i386.deb

Size/MD5 checksum: 79892 7460f7b76d597bcb02bdc0fe5897a32a

http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2_1.2.7-4etch3_i386.deb

Size/MD5 checksum: 86674 aebef9f4a309afdf01a7cce17b6f57b

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-dbg_1.2.7-4etch3_i386.deb

Size/MD5 checksum: 997608 e754dc8df237302fac7019754e42352b

http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2-dev_1.2.7-4etch3_i386.deb

Size/MD5 checksum: 53418 b45cf2a324d52524244351d213c8be41

http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2-dev_1.2.7-4etch3_i386.deb

Size/MD5 checksum: 137686 b726701fdb3e8948e5111e2e831bf853

http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2_1.2.7-4etch3_i386.deb

Size/MD5 checksum: 160080 c029e686ec624c2fdf156f885d1daf5c

ia64 architecture (Intel ia64)

http://security.debian.org/pool/updates/main/c/cupsys/cupsys_1.2.7-4etch3_ia64.deb

Size/MD5 checksum: 1770478 73e7565983c31c3e651dd55acb38c0c7

http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2_1.2.7-4etch3_ia64.deb

Size/MD5 checksum: 203722 9d2b9b9d1c3999a3f4ccf7e5e446bd1a

[SECURITY] [DSA 1530-1] New cupsys packages fix multiple vulnerabilities

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-dbg_1.2.7-4etch3_ia64.deb
Size/MD5 checksum: 1107480 d0898394febd60b7bf80e1e4ff335a39
http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2-dev_1.2.7-4etch3_ia64.deb
Size/MD5 checksum: 73934 5156c8db255299aa66053bb4415cde19
http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2_1.2.7-4etch3_ia64.deb
Size/MD5 checksum: 106208 db2ad0519d15ee795758f72b3c093068
http://security.debian.org/pool/updates/main/c/cupsys/cupsys-client_1.2.7-4etch3_ia64.deb
Size/MD5 checksum: 106220 8228fb0ccf8cc888973731f2aa72c8c4
http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2-dev_1.2.7-4etch3_ia64.deb
Size/MD5 checksum: 192358 c1ee340a3e893b3f22adb138923167c2
http://security.debian.org/pool/updates/main/c/cupsys/cupsys-bsd_1.2.7-4etch3_ia64.deb
Size/MD5 checksum: 46324 771aaa1b244d01eacdd62e8e963d434f

mips architecture (MIPS (Big Endian))

http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2_1.2.7-4etch3_mips.deb
Size/MD5 checksum: 86208 03d9d365f1c41e2efc36fc1a19dcb813
http://security.debian.org/pool/updates/main/c/cupsys/cupsys-dbg_1.2.7-4etch3_mips.deb
Size/MD5 checksum: 1096636 65217c4fc57a23e065c9da14dfad6c9d
http://security.debian.org/pool/updates/main/c/cupsys/cupsys_1.2.7-4etch3_mips.deb
Size/MD5 checksum: 1567240 46f2194418cb1d5800c44ae13bcd51ee
http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2-dev_1.2.7-4etch3_mips.deb
Size/MD5 checksum: 57520 02e313bad869d4c50a6dde506765633b
http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2_1.2.7-4etch3_mips.deb
Size/MD5 checksum: 157528 f42c10ade950e4faa4403da4e8d740c4
http://security.debian.org/pool/updates/main/c/cupsys/cupsys-client_1.2.7-4etch3_mips.deb
Size/MD5 checksum: 76156 d4778055a8900dcb6eaf2100a8172b63
http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2-dev_1.2.7-4etch3_mips.deb
Size/MD5 checksum: 150976 5c00fd263eb81453450af5d5e79fe5b4
http://security.debian.org/pool/updates/main/c/cupsys/cupsys-bsd_1.2.7-4etch3_mips.deb
Size/MD5 checksum: 36114 4ba209d715050a942d0c9025869378fe

mipsel architecture (MIPS (Little Endian))

http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2_1.2.7-4etch3_mipsel.deb
Size/MD5 checksum: 86404 41a26e5e4196385e67dddee0337c0ade
http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2_1.2.7-4etch3_mipsel.deb
Size/MD5 checksum: 158050 1b5af4a50dcfe41ec2b35af9a47d40b3
http://security.debian.org/pool/updates/main/c/cupsys/cupsys-bsd_1.2.7-4etch3_mipsel.deb
Size/MD5 checksum: 36060 09d1cfd7b2e925b3f846d22cf760ba11
http://security.debian.org/pool/updates/main/c/cupsys/cupsys_1.2.7-4etch3_mipsel.deb
Size/MD5 checksum: 1552652 67cf88cac0c510bec526c49025d7cbe0
http://security.debian.org/pool/updates/main/c/cupsys/cupsys-dbg_1.2.7-4etch3_mipsel.deb
Size/MD5 checksum: 1084290 082931629866ea5a6aba940997698af7
http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2-dev_1.2.7-4etch3_mipsel.deb
Size/MD5 checksum: 57694 6e120d7fc4a6643eb208333b30e7c5c9
http://security.debian.org/pool/updates/main/c/cupsys/cupsys-client_1.2.7-4etch3_mipsel.deb
Size/MD5 checksum: 77448 f411d88639ee78a68d46ece45e91368f
http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2-dev_1.2.7-4etch3_mipsel.deb
Size/MD5 checksum: 150900 09be1543e6cd767098a3af2a70791036

[SECURITY] [DSA 1530-1] New cupsys packages fix multiple vulnerabilities

powerpc architecture (PowerPC)

http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2-dev_1.2.7-4etch3_powerpc.deb

Size/MD5 checksum: 136866 623ea75ab7f6603f9ddc9276389c90ea

http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2_1.2.7-4etch3_powerpc.deb

Size/MD5 checksum: 162686 5766c22ea9cad4f8e5acbf8dd6ad48f6

http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2_1.2.7-4etch3_powerpc.deb

Size/MD5 checksum: 87910 767921a7b2ed329a3107da1f0dbb7dda

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-bsd_1.2.7-4etch3_powerpc.deb

Size/MD5 checksum: 41298 875908633ca26db04739a334b03c42c2

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-client_1.2.7-4etch3_powerpc.deb

Size/MD5 checksum: 89998 0c81d4c99f07d7b0cdd91a2a9a6ad28

http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2-dev_1.2.7-4etch3_powerpc.deb

Size/MD5 checksum: 51788 87423f593d57c4c9d0cc80cfafa28f87

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-dbg_1.2.7-4etch3_powerpc.deb

Size/MD5 checksum: 1142146 6c4479057269b64596d123d5cf859747

http://security.debian.org/pool/updates/main/c/cupsys/cupsys_1.2.7-4etch3_powerpc.deb

Size/MD5 checksum: 1575696 eb08aafdd1c60d707b874a31dcab67b4

s390 architecture (IBM S/390)

http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2_1.2.7-4etch3_s390.deb

Size/MD5 checksum: 166184 d748308d0a477ad16a42e25671f49dd9

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-bsd_1.2.7-4etch3_s390.deb

Size/MD5 checksum: 37422 6a3f5390f4ff82bd1c8ef4d64f0fcc46

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-dbg_1.2.7-4etch3_s390.deb

Size/MD5 checksum: 1036106 08ad799adaeb1ccd9538048e685d69d6

http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2_1.2.7-4etch3_s390.deb

Size/MD5 checksum: 87194 e881e70f5b31b800989f14fd4e97368f

http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2-dev_1.2.7-4etch3_s390.deb

Size/MD5 checksum: 52256 ec508d448806c889b0c79aed8d95cc3e

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-client_1.2.7-4etch3_s390.deb

Size/MD5 checksum: 82340 c9ab3bc26da68abdde50d365b4224434

http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2-dev_1.2.7-4etch3_s390.deb

Size/MD5 checksum: 144934 61cf1f32851be64340ffb36b266ee0a7

http://security.debian.org/pool/updates/main/c/cupsys/cupsys_1.2.7-4etch3_s390.deb

Size/MD5 checksum: 1586624 1921d0bc3b7b03d4ed952ecb4b0b561b

sparc architecture (Sun SPARC/UltraSPARC)

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-client_1.2.7-4etch3_sparc.deb

Size/MD5 checksum: 78500 74d7872d04914d26d5a4baa768437603

http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2-dev_1.2.7-4etch3_sparc.deb

Size/MD5 checksum: 51572 93fd782dbbc7148c9f96b18ad7ebe111

http://security.debian.org/pool/updates/main/c/cupsys/libcupsimage2_1.2.7-4etch3_sparc.deb

Size/MD5 checksum: 84622 6eb7012156c87266af9802d38f1dd366

http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2_1.2.7-4etch3_sparc.deb

Size/MD5 checksum: 158596 68ca94de2c329c162ae40ac5b79af29b

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-bsd_1.2.7-4etch3_sparc.deb

Size/MD5 checksum: 36018 61ffbc960bea5c6fda52ffefa8886b7

http://security.debian.org/pool/updates/main/c/cupsys/cupsys-dbg_1.2.7-4etch3_sparc.deb

[SECURITY] [DSA 1530-1] New cupsys packages fix multiple vulnerabilities

Size/MD5 checksum: 991000 3135666aadf8d4f4cd273fbd7d50cfca

http://security.debian.org/pool/updates/main/c/cupsys/libcupsys2-dev_1.2.7-4etch3_sparc.deb

Size/MD5 checksum: 139570 e281ec84c08bcac3f54d5017b6917e0b

http://security.debian.org/pool/updates/main/c/cupsys/cupsys_1.2.7-4etch3_sparc.deb

Size/MD5 checksum: 1561792 21cd9a3e1e89ba96aa11890858194b82

These files will probably be moved into the stable distribution on its next update.

-

For apt-get: deb <http://security.debian.org/stable/updates/main>

For dpkg-ftp: [ftp://security.debian.org/debian-security dists/stable/updates/main](ftp://security.debian.org/debian-security/dists/stable/updates/main)

Mailing list: debian-security-announce@xxxxxxxxxxxxxxxxxxx

Package info: `apt-cache show <pkg>' and <http://packages.debian.org/<pkg>>

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.6 (GNU/Linux)

iD8DBQFH6RVAYrVLjBFATsMRAozSAJ9kTMEJ+adGZ1Sn0N6kOyhCmJU0HACeK7Xp

2NTRUT1F1Cu9Xrm9EGvmg3M=

=Fgu/

-----END PGP SIGNATURE-----