

[Full-disclosure] [USN-166-1] Evolution vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-08/0364.html>

From: Martin Pitt (martin.pitt_at_canonical.com)

Date: 08/11/05

Date: Thu, 11 Aug 2005 15:26:49 +0200

To: ubuntu-security-announce@lists.ubuntu.com

=====
Ubuntu Security Notice USN-166-1 August 11, 2005

evolution vulnerabilities

<http://lists.grok.org.uk/pipermail/full-disclosure/2005-August/035922.html>

CAN-2005-0806
=====

A security issue affects the following Ubuntu releases:

Ubuntu 4.10 (Warty Warthog)

Ubuntu 5.04 (Hoary Hedgehog)

The following packages are affected:

evolution

The problem can be corrected by upgrading the affected package to version 2.0.2-0ubuntu2.3 (for Ubuntu 4.10), or 2.2.1.1-0ubuntu4.2 (for Ubuntu 5.04). After performing a standard system upgrade you need to restart Evolution to effect the necessary changes.

Details follow:

Ulf Harnhammar discovered several format string vulnerabilities in Evolution. By tricking an user into viewing a specially crafted vCard attached to an email, specially crafted contact data from an LDAP server, specially crafted task lists from remote servers, or saving Calendar entries with this malicious task list data, it was possible for an attacker to execute arbitrary code with the privileges of the user running Evolution.

In addition, this update fixes a Denial of Service vulnerability in the mail attachment parser. This could be exploited to crash Evolution

Full-Disclosure: [Full-disclosure] [USN-166-1] Evolution vulnerabilities

by tricking an user into opening a malicious email with a specially crafted attachment file name. This does only affect the Ubuntu 4.10 version, the Evolution package shipped with Ubuntu 5.04 is not affected. (CAN-2005-0806)

Updated packages for Ubuntu 4.10 (Warty Warthog):

Source archives:

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution_2.0.2-0ubuntu2.3.diff.gz

Size/MD5: 52759 1c1f04dc9cd0710f3a61faf0dd029e79

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution_2.0.2-0ubuntu2.3.dsc

Size/MD5: 1186 74a30392895280e6829a2c2ca2b212ec

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution_2.0.2.orig.tar.gz

Size/MD5: 20925198 7b3c1b6b7f67c548d7e45bf2ed7abd0f

Architecture independent packages:

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution1.5-dev_2.0.2-0ubuntu2.3_all.deb

Size/MD5: 16794 ab6b14f3a175d166c0e47720f0731f40

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution1.5_2.0.2-0ubuntu2.3_all.deb

Size/MD5: 39842 a8064117dd789bdc66d3c5b003d55cbb

amd64 architecture (Athlon64, Opteron, EM64T Xeon)

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution-dev_2.0.2-0ubuntu2.3_amd64.deb

Size/MD5: 134350 2211b891401b73156d2b27037e20715d

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution_2.0.2-0ubuntu2.3_amd64.deb

Size/MD5: 10437964 50dc08b0993bb3cdb5a8c4f25f775e33

i386 architecture (x86 compatible Intel/AMD)

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution-dev_2.0.2-0ubuntu2.3_i386.deb

Size/MD5: 134366 7fec365de11d7868a18ee4f1be6d5eff

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution_2.0.2-0ubuntu2.3_i386.deb

Size/MD5: 10201990 4e470ac7010cd86183839eedffe77d67

powerpc architecture (Apple Macintosh G3/G4/G5)

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution-dev_2.0.2-0ubuntu2.3_powerpc.deb

Size/MD5: 134380 1288cb986f1adfb48abef126b006e1f

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution_2.0.2-0ubuntu2.3_powerpc.deb

Size/MD5: 10255086 e1cf172b8b249d25ddad83a5814397b7

Updated packages for Ubuntu Ubuntu 5.04 (Hoary Hedgehog):

Source archives:

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution_2.2.1.1-0ubuntu4.2.diff.gz

Size/MD5: 16398 749d47606d267a13fba5b178eb228063

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution_2.2.1.1-0ubuntu4.2.dsc

Full-Disclosure: [Full-disclosure] [USN-166-1] Evolution vulnerabilities

Size/MD5: 1244 c5a54e2bd7d7e83eedecf2d244f0018d

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution_2.2.1.1.orig.tar.gz

Size/MD5: 18423287 8a0e435c05b50fe2d7d7bea8c1d5c7b84

amd64 architecture (Athlon64, Opteron, EM64T Xeon)

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution-dev_2.2.1.1-0ubuntu4.2_amd64.deb

Size/MD5: 106666 31a1d051cdaaf3f5f902cbb4a380ffd5

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution_2.2.1.1-0ubuntu4.2_amd64.deb

Size/MD5: 4393034 e3e161af68ebb6061884f94517abe1ef

i386 architecture (x86 compatible Intel/AMD)

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution-dev_2.2.1.1-0ubuntu4.2_i386.deb

Size/MD5: 106660 697e4fdf746df3ea8a72fb2bd22987fe

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution_2.2.1.1-0ubuntu4.2_i386.deb

Size/MD5: 4211180 7487a4feb64c082574988f8390c732c3

powerpc architecture (Apple Macintosh G3/G4/G5)

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution-dev_2.2.1.1-0ubuntu4.2_powerpc.deb

Size/MD5: 106660 6a72027f985938c70837a509e3948c8a

http://security.ubuntu.com/ubuntu/pool/main/e/evolution/evolution_2.2.1.1-0ubuntu4.2_powerpc.deb

Size/MD5: 4289442 f09870fb174824247038d32ce62c965e

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

- application/pgp-signature attachment: [Digital signature](#)