

[Full-disclosure] [SECURITY] [DSA 1439-1] New typo3-src packages fix SQL injection

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-12/msg00604.html>

- *From:* Thijs Kinkhorst <thijs@xxxxxxxxxx>
 - *Date:* Fri, 28 Dec 2007 16:41:20 +0100
-

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

Hash: SHA1

Debian Security Advisory DSA-1439-1 security@xxxxxxxxxx
<http://www.debian.org/security/> Thijs Kinkhorst
December 28, 2007 <http://www.debian.org/security/faq>

Package : typo3-src
Vulnerability : missing input sanitising
Problem-Type : remote
Debian-specific: no
CVE ID : CVE-2007-6381
Debian Bug : 457446

Henning Pingel discovered that TYPO3, a web content management framework, performs insufficient input sanitising, making it vulnerable to SQL injection by logged-in backend users.

For the stable distribution (etch), this problem has been fixed in version typo3-src 4.0.2+debian-4.

The old stable distribution (sarge) doesn't contain typo3-src.

For the unstable distribution (sid) and for the testing distribution (lenny), this problem has been fixed in version 4.1.5-1.

We recommend that you upgrade your typo3-src packages.

Upgrade instructions

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

[Full-disclosure] [SECURITY] [DSA 1439-1] New typo3-src packages fix SQL injection

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 4.0 (stable)

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

Source archives:

```
http://security.debian.org/pool/updates/main/t/typo3-src/typo3-src\_4.0.2+debian-4.diff.gz
Size/MD5 checksum: 13795 c88de483225fb01726b21b1c5c6754da
http://security.debian.org/pool/updates/main/t/typo3-src/typo3-src\_4.0.2+debian.orig.tar.gz
Size/MD5 checksum: 7683527 be509391b0e4d24278c14100c09dc673
http://security.debian.org/pool/updates/main/t/typo3-src/typo3-src\_4.0.2+debian-4.dsc
Size/MD5 checksum: 902 faf88b5c6ae931fb4ce919a9e8c501c4
```

Architecture independent packages:

```
http://security.debian.org/pool/updates/main/t/typo3-src/typo3\_4.0.2+debian-4\_all.deb
Size/MD5 checksum: 76268 2004e720cca629d8e29c0689ad4ca5b8
http://security.debian.org/pool/updates/main/t/typo3-src/typo3-src-4.0\_4.0.2+debian-4\_all.deb
Size/MD5 checksum: 7686574 c7da1b1f0f98ce3e3ed98cf46fe71ba4
```

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
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)

```
iD8DBQFHdRjTXm3vHE4uyloRAmBZAJ93cWZ7ErHiI4k3AjItEdA98qXx6wCgmNJ1
E2Cllaa0gTQgaiS2lXavrrY=
```

=pbJ3

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

Full-Disclosure – We believe in it.

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

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