

[Full-disclosure] MDKSA-2005:170 – Updated mozilla packages fix multiple vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-09/0708.html>

From: Mandriva Security Team (security_at_mandriva.com)

Date: 09/27/05

To: full-disclosure@lists.grok.org.uk

Date: Mon, 26 Sep 2005 21:55:24 -0600

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

Hash: SHA1

Mandriva Linux Security Update Advisory

Package name: mozilla

Advisory ID: MDKSA-2005:170

Date: September 26th, 2005

Affected versions: 10.1, Corporate 3.0

Problem Description:

A number of vulnerabilities have been discovered in Mozilla that have been corrected in version 1.7.12:

A bug in the way Mozilla processes XBM images could be used to execute arbitrary code via a specially crafted XBM image file (CAN-2005-2701).

A bug in the way Mozilla handles certain Unicode sequences could be used to execute arbitrary code via viewing a specially crafted Unicode sequence (CAN-2005-2702).

A bug in the way Mozilla makes XMLHttpRequests could be abused by a malicious web page to exploit other proxy or server flaws from the victim's machine; however, the default behaviour of the browser is to disallow this (CAN-2005-2703).

A bug in the way Mozilla implemented its XBL interface could be abused by a malicious web page to create an XBL binding in such a way as to allow arbitrary JavaScript execution with chrome permissions

Full-Disclosure: [Full-disclosure] MDKSA-2005:170 – Updated mozilla packages fix multiple vulnerabilities

(CAN-2005-2704).

An integer overflow in Mozilla's JavaScript engine could be manipulated in certain conditions to allow a malicious web page to execute arbitrary code (CAN-2005-2705).

A bug in the way Mozilla displays about: pages could be used to execute JavaScript with chrome privileges (CAN-2005-2706).

A bug in the way Mozilla opens new windows could be used by a malicious web page to construct a new window without any user interface elements (such as address bar and status bar) that could be used to potentially mislead the user (CAN-2005-2707).

The updated packages have been patched to address these issues and all users are urged to upgrade immediately.

References:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2701>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2702>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2703>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2704>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2705>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2706>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2707>
<http://www.mozilla.org/security/announce/mfsa2005-58.html>

Updated Packages:

Mandrakelinux 10.1:

98862a59fbf6d6eb5db05dd89cdd7a56 10.1/RPMS/libnspr4-1.7.8-0.3.101mdk.i586.rpm
7b75d7436ddc167dc64b5361fbdf6851 10.1/RPMS/libnspr4-devel-1.7.8-0.3.101mdk.i586.rpm
9e8eb18bea99ae419f5a1cab5ffef6b2 10.1/RPMS/libnss3-1.7.8-0.3.101mdk.i586.rpm
7427a69600ffffa87f60603b3c603935 10.1/RPMS/libnss3-devel-1.7.8-0.3.101mdk.i586.rpm
fe4003cfd5775a11a789dbb56282cea6 10.1/RPMS/mozilla-1.7.8-0.3.101mdk.i586.rpm
b66c918e364a92ed461e598164adac76 10.1/RPMS/mozilla-devel-1.7.8-0.3.101mdk.i586.rpm
1b5d1b456686b187ae7c3388a9591247 10.1/RPMS/mozilla-dom-inspector-1.7.8-0.3.101mdk.i586.rpm
839c117682b0d888963511e88eaba2e9 10.1/RPMS/mozilla-enigmail-1.7.8-0.3.101mdk.i586.rpm
a11a7c6afcb7c3fd2044c8b2f9a8bbc2 10.1/RPMS/mozilla-enigmime-1.7.8-0.3.101mdk.i586.rpm
53eb2dc1a62352b2e17438c89418c527 10.1/RPMS/mozilla-irc-1.7.8-0.3.101mdk.i586.rpm
0c249773876d3b8bf77c675f897bb6ff 10.1/RPMS/mozilla-js-debugger-1.7.8-0.3.101mdk.i586.rpm
f6cfd1650616de8edf2c158ca8648c56 10.1/RPMS/mozilla-mail-1.7.8-0.3.101mdk.i586.rpm
f521e0837986889581f026f734d1703f 10.1/RPMS/mozilla-spellchecker-1.7.8-0.3.101mdk.i586.rpm
5c5d9bcb713136927980c374d8719ed4 10.1/SRPMS/mozilla-1.7.8-0.3.101mdk.src.rpm

Mandrakelinux 10.1/X86_64:

ce6e99481e523896aea8cc1e91c51523 x86_64/10.1/RPMS/lib64nspr4-1.7.8-0.3.101mdk.x86_64.rpm
fadccb049a886a1ddf8cf03920ea120f x86_64/10.1/RPMS/lib64nspr4-devel-1.7.8-0.3.101mdk.x86_64.rpm

Full-Disclosure: [Full-disclosure] MDKSA-2005:170 – Updated mozilla packages fix multiple vulnerabilities

98862a59fbf6d6eb5db05dd89cdd7a56 x86_64/10.1/RPMS/libnspr4-1.7.8-0.3.101mdk.i586.rpm
df7c4331144029e67bd9493571626aff x86_64/10.1/RPMS/lib64nss3-1.7.8-0.3.101mdk.x86_64.rpm
bdd269e07644d46d4e380878bf0746e8 x86_64/10.1/RPMS/lib64nss3-devel-1.7.8-0.3.101mdk.x86_64.rpm
9e8eb18bea99ae419f5a1cab5ffef6b2 x86_64/10.1/RPMS/libnss3-1.7.8-0.3.101mdk.i586.rpm
da3d352c690a7fc91cb83dc49819cd2a x86_64/10.1/RPMS/mozilla-1.7.8-0.3.101mdk.x86_64.rpm
b13b4dc501a6eff651a4ef6d3b371b44 x86_64/10.1/RPMS/mozilla-devel-1.7.8-0.3.101mdk.x86_64.rpm
5b13733c766009ebfd0aca606ac224f2
x86_64/10.1/RPMS/mozilla-dom-inspector-1.7.8-0.3.101mdk.x86_64.rpm
3dfab88b55900580d0588fd7c8a6e219
x86_64/10.1/RPMS/mozilla-enigmail-1.7.8-0.3.101mdk.x86_64.rpm
e5892c4a8bd56b4a9cea3e8e21bc83b5
x86_64/10.1/RPMS/mozilla-enigmime-1.7.8-0.3.101mdk.x86_64.rpm
84946972d12ce8109d41f9bbcc99a796 x86_64/10.1/RPMS/mozilla-irc-1.7.8-0.3.101mdk.x86_64.rpm
ee060262c82cd51501b9645d9bb93c91
x86_64/10.1/RPMS/mozilla-js-debugger-1.7.8-0.3.101mdk.x86_64.rpm
30cfa0281f3f6a2b6d25bfb1132f7b0d x86_64/10.1/RPMS/mozilla-mail-1.7.8-0.3.101mdk.x86_64.rpm
fb3f368becb9ebe11c16dd41a299e59a
x86_64/10.1/RPMS/mozilla-spellchecker-1.7.8-0.3.101mdk.x86_64.rpm
5c5d9bcb713136927980c374d8719ed4 x86_64/10.1/SRPMS/mozilla-1.7.8-0.3.101mdk.src.rpm

Corporate 3.0:

4d292376b2e472f830b5f4aa42068909 corporate/3.0/RPMS/libnspr4-1.7.8-0.3.C30mdk.i586.rpm
be7ea7688875e5fe4ebed3c2102e8dfa corporate/3.0/RPMS/libnspr4-devel-1.7.8-0.3.C30mdk.i586.rpm
1a2e78d8bc3730ee5247566cf9f6e451 corporate/3.0/RPMS/libnss3-1.7.8-0.3.C30mdk.i586.rpm
8da9e0004e40168e2d14123d03ed412e corporate/3.0/RPMS/libnss3-devel-1.7.8-0.3.C30mdk.i586.rpm
1a9ae203c7a92f7b28ed492b1a5b409f corporate/3.0/RPMS/mozilla-1.7.8-0.3.C30mdk.i586.rpm
5c962618de8f8f32d51d408b9512e159 corporate/3.0/RPMS/mozilla-devel-1.7.8-0.3.C30mdk.i586.rpm
b455b06389295360aca3d2d425b37167
corporate/3.0/RPMS/mozilla-dom-inspector-1.7.8-0.3.C30mdk.i586.rpm
6545f2c00a2945b4876809e640af477f corporate/3.0/RPMS/mozilla-enigmail-1.7.8-0.3.C30mdk.i586.rpm
484a08328be60b82fd7da351cfd2b27c corporate/3.0/RPMS/mozilla-enigmime-1.7.8-0.3.C30mdk.i586.rpm
12485fa965a7d7e16b9499a049fa32d1 corporate/3.0/RPMS/mozilla-irc-1.7.8-0.3.C30mdk.i586.rpm
651c02d92b878bbe72c3fb014928aad3
corporate/3.0/RPMS/mozilla-js-debugger-1.7.8-0.3.C30mdk.i586.rpm
0e691e34a0507e43cc40290f4ee00664 corporate/3.0/RPMS/mozilla-mail-1.7.8-0.3.C30mdk.i586.rpm
fc6fe3d8752b7fc011a9b423acbedddf
corporate/3.0/RPMS/mozilla-spellchecker-1.7.8-0.3.C30mdk.i586.rpm
63155b5fb6b43c0058cf1ca880707271 corporate/3.0/SRPMS/mozilla-1.7.8-0.3.C30mdk.src.rpm

Corporate 3.0/X86_64:

bd7d2846823a5988f742d1a90b82592e
x86_64/corporate/3.0/RPMS/lib64nspr4-1.7.8-0.3.C30mdk.x86_64.rpm
f1e0909cca43f58ee6a27f29f6347ee1
x86_64/corporate/3.0/RPMS/lib64nspr4-devel-1.7.8-0.3.C30mdk.x86_64.rpm
b753668e90a44fbcad600fbaf0375323
x86_64/corporate/3.0/RPMS/lib64nss3-1.7.8-0.3.C30mdk.x86_64.rpm
0859991a0652bfa39041f7d8391ddca3
x86_64/corporate/3.0/RPMS/lib64nss3-devel-1.7.8-0.3.C30mdk.x86_64.rpm
e88886fad7ac2d94725a00df8674da33 x86_64/corporate/3.0/RPMS/mozilla-1.7.8-0.3.C30mdk.x86_64.rpm
1c3f3ae94e4479b1f57645be562c060b
x86_64/corporate/3.0/RPMS/mozilla-devel-1.7.8-0.3.C30mdk.x86_64.rpm

Full-Disclosure: [Full-disclosure] MDKSA-2005:170 – Updated mozilla packages fix multiple vulnerabilities

```
2d7875c006f17c48c19487ca60891ec3
x86_64/corporate/3.0/RPMS/mozilla-dom-inspector-1.7.8-0.3.C30mdk.x86_64.rpm
5018aa698bd6007b886da4c87e15a675
x86_64/corporate/3.0/RPMS/mozilla-enigmail-1.7.8-0.3.C30mdk.x86_64.rpm
22d583ca004e599529dc205cce7dec75
x86_64/corporate/3.0/RPMS/mozilla-enigmime-1.7.8-0.3.C30mdk.x86_64.rpm
42edd5f3f1ff285f3995e2e8dec60c58
x86_64/corporate/3.0/RPMS/mozilla-irc-1.7.8-0.3.C30mdk.x86_64.rpm
d7a2e219ad7d083cd174268322e91bfe
x86_64/corporate/3.0/RPMS/mozilla-js-debugger-1.7.8-0.3.C30mdk.x86_64.rpm
408444bc05b4e98c9f478651f66101a5
x86_64/corporate/3.0/RPMS/mozilla-mail-1.7.8-0.3.C30mdk.x86_64.rpm
bba893fa0db446e56405ca330e417f23
x86_64/corporate/3.0/RPMS/mozilla-spellchecker-1.7.8-0.3.C30mdk.x86_64.rpm
63155b5fb6b43c0058cf1ca880707271 x86_64/corporate/3.0/SRPMS/mozilla-1.7.8-0.3.C30mdk.src.rpm
```

To upgrade automatically use MandrakeUpdate or urpmi. The verification of md5 checksums and GPG signatures is performed automatically for you.

All packages are signed by Mandriva for security. You can obtain the GPG public key of the Mandriva Security Team by executing:

```
gpg --recv-keys --keyserver pgp.mit.edu 0x22458A98
```

You can view other update advisories for Mandriva Linux at:

<http://www.mandriva.com/security/advisories>

If you want to report vulnerabilities, please contact

security_(at)_mandriva.com

```
Type Bits/KeyID Date User ID
pub 1024D/22458A98 2000-07-10 Mandriva Security Team
<security*mandriva.com>
```

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

Version: GnuPG v1.2.4 (GNU/Linux)

```
iD8DBQFDOMKsmqjQ0CJFipgRAi+OAJ4ugLy8iwhAfSvKKjVtqqqpf26EgCgiqI3
IRMnADOTrn7+7O5pL6VkyzE=
=3897
```

-----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/>