

# [ MDVSA-2008:045 ] – Updated MPlayer packages fix a few vulnerabilities

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-02/msg00230.html>

---

- *From:* [security@xxxxxxxxxxxx](mailto:security@xxxxxxxxxxxx)
  - *Date:* Thu, 14 Feb 2008 16:49:40 -0700
- 

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

Hash: SHA1

---

Mandriva Linux Security Advisory MDVSA-2008:045  
<http://www.mandriva.com/security/>

---

Package : mplayer  
Date : February 14, 2008  
Affected: 2007.1, 2008.0, Corporate 3.0

---

## Problem Description:

Heap-based buffer overflow in the `rmff_dump_cont` function in `input/libreal/rmff.c` in `xine-lib 1.1.9` and earlier allows remote attackers to execute arbitrary code via the SDP Abstract attribute, related to the `rmff_dump_header` function and related to disregarding the `max` field. Although originally a `xine-lib` issue, also affects MPlayer due to code similarity. (CVE-2008-0225)

Multiple heap-based buffer overflows in the `rmff_dump_cont` function in `input/libreal/rmff.c` in `xine-lib 1.1.9` allow remote attackers to execute arbitrary code via the SDP (1) Title, (2) Author, or (3) Copyright attribute, related to the `rmff_dump_header` function, different vectors than CVE-2008-0225. Although originally a `xine-lib` issue, also affects MPlayer due to code similarity. (CVE-2008-0238)

Array index error in `libmpdemux/demux_mov.c` in MPlayer 1.0 rc2 and earlier might allow remote attackers to execute arbitrary code via a QuickTime MOV file with a crafted `stsc atom` tag. (CVE-2008-0485)

Array index vulnerability in `libmpdemux/demux_audio.c` in MPlayer 1.0rc2 and SVN before r25917, and possibly earlier versions, as used in `Xine-lib 1.1.10`, might allow remote attackers to execute

## [ MDVSA-2008:045 ] – Updated MPlayer packages fix a few vulnerabilities

arbitrary code via a crafted FLAC tag, which triggers a buffer overflow. (CVE-2008-0486)

Buffer overflow in stream\_cddb.c in MPlayer 1.0rc2 and SVN before r25824 allows remote user-assisted attackers to execute arbitrary code via a Cddb database entry containing a long album title. (CVE-2008-0629)

Buffer overflow in url.c in MPlayer 1.0rc2 and SVN before r25823 allows remote attackers to execute arbitrary code via a crafted URL that prevents the IPv6 parsing code from setting a pointer to NULL, which causes the buffer to be reused by the unescape code. (CVE-2008-0630)

The updated packages have been patched to prevent these issues.

---

### References:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0225>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0238>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0485>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0486>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0629>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0630>

---

### Updated Packages:

#### Mandriva Linux 2007.1:

bc4d94bebd6e6d3f5ae8939c2a6eae17 2007.1/i586/libdha1.0-1.0-1.rc1.11.5mdv2007.1.i586.rpm  
7b01d664225bcb1bd474dfd97d3e50a3 2007.1/i586/mencoder-1.0-1.rc1.11.5mdv2007.1.i586.rpm  
b1258431ee88be325c9c407b0ae238ae 2007.1/i586/mplayer-1.0-1.rc1.11.5mdv2007.1.i586.rpm  
9ac91fe253b625a24f03613912eaf905 2007.1/i586/mplayer-doc-1.0-1.rc1.11.5mdv2007.1.i586.rpm  
e674dc2f80cfb01a3d58e1f323bf028e 2007.1/i586/mplayer-gui-1.0-1.rc1.11.5mdv2007.1.i586.rpm  
f6c93fbb2298603dcadfcc199e920f4c 2007.1/SRPMS/mplayer-1.0-1.rc1.11.5mdv2007.1.src.rpm

#### Mandriva Linux 2007.1/X86\_64:

8e8356ef4f1d82350b2ec4603e9c97ab 2007.1/x86\_64/mencoder-1.0-1.rc1.11.5mdv2007.1.x86\_64.rpm  
24cbb105fc1b2d538a291635af1175f5 2007.1/x86\_64/mplayer-1.0-1.rc1.11.5mdv2007.1.x86\_64.rpm  
270d9a22d97b311808be80b25b9e0d46 2007.1/x86\_64/mplayer-doc-1.0-1.rc1.11.5mdv2007.1.x86\_64.rpm  
b895f7c06b55b182aef4a077f842574f 2007.1/x86\_64/mplayer-gui-1.0-1.rc1.11.5mdv2007.1.x86\_64.rpm  
f6c93fbb2298603dcadfcc199e920f4c 2007.1/SRPMS/mplayer-1.0-1.rc1.11.5mdv2007.1.src.rpm

#### Mandriva Linux 2008.0:

f58551219080f3ac3893b996276e24e0 2008.0/i586/libdha1.0-1.0-1.rc1.20.2mdv2008.0.i586.rpm  
edc7b645e0da4e96761cfb4277f00e3d 2008.0/i586/mencoder-1.0-1.rc1.20.2mdv2008.0.i586.rpm  
2b89bc02908f421c2e18771abbb009a0 2008.0/i586/mplayer-1.0-1.rc1.20.2mdv2008.0.i586.rpm  
e9ec1a063f1b0f6e63efbfc14c65f95e 2008.0/i586/mplayer-doc-1.0-1.rc1.20.2mdv2008.0.i586.rpm  
b43c4c4705f12fad0c612f188b84f3ba 2008.0/i586/mplayer-gui-1.0-1.rc1.20.2mdv2008.0.i586.rpm  
5776eb9afddc671d323ca44c8b7d3efb 2008.0/SRPMS/mplayer-1.0-1.rc1.20.2mdv2008.0.src.rpm

[ MDVSA-2008:045 ] – Updated MPlayer packages fix a few vulnerabilities

Mandriva Linux 2008.0/X86\_64:

e5f6acd329239d27ba4e89300d54046d 2008.0/x86\_64/mencoder-1.0-1.rc1.20.2mdv2008.0.x86\_64.rpm  
8af0e97fa75444467bb187ba73f0fa14 2008.0/x86\_64/mplayer-1.0-1.rc1.20.2mdv2008.0.x86\_64.rpm  
3fa2fd143c74b1210bf8d49b22e3996f 2008.0/x86\_64/mplayer-doc-1.0-1.rc1.20.2mdv2008.0.x86\_64.rpm  
fd53467bec0513eab96b672777c5a0c5 2008.0/x86\_64/mplayer-gui-1.0-1.rc1.20.2mdv2008.0.x86\_64.rpm  
5776eb9afddc671d323ca44c8b7d3efb 2008.0/SRPMS/mplayer-1.0-1.rc1.20.2mdv2008.0.src.rpm

Corporate 3.0:

65ce689c4bdc14b5ae19697ea685b469 corporate/3.0/i586/libdha0.1-1.0-0.pre3.14.14.C30mdk.i586.rpm  
908d34d7373434280d7e384745f11509 corporate/3.0/i586/libpostproc0-1.0-0.pre3.14.14.C30mdk.i586.rpm  
9394b4a56ac7879785ba3ba3b40cf2e4  
corporate/3.0/i586/libpostproc0-devel-1.0-0.pre3.14.14.C30mdk.i586.rpm  
07b4ed8181c85011191d4536f8972654 corporate/3.0/i586/mencoder-1.0-0.pre3.14.14.C30mdk.i586.rpm  
6b9be8b56f7f375c3bba37786e015ce3 corporate/3.0/i586/mplayer-1.0-0.pre3.14.14.C30mdk.i586.rpm  
5bb8239d3f5a93bd3b5fb6be9015b99b corporate/3.0/i586/mplayer-gui-1.0-0.pre3.14.14.C30mdk.i586.rpm  
dd4f44dc8d0aa181b7ce3c5be006ef21 corporate/3.0/SRPMS/mplayer-1.0-0.pre3.14.14.C30mdk.src.rpm

Corporate 3.0/X86\_64:

3be2677a831513f23e3c223f2c0b1988  
corporate/3.0/x86\_64/lib64postproc0-1.0-0.pre3.14.14.C30mdk.x86\_64.rpm  
ef16b06b058c39529edfdb4904bfa017  
corporate/3.0/x86\_64/lib64postproc0-devel-1.0-0.pre3.14.14.C30mdk.x86\_64.rpm  
2c21398a4ca6d86f6bb464b3f4bab6bf  
corporate/3.0/x86\_64/mencoder-1.0-0.pre3.14.14.C30mdk.x86\_64.rpm  
c9b10c36682298ba5e62ec9509ed5593 corporate/3.0/x86\_64/mplayer-1.0-0.pre3.14.14.C30mdk.x86\_64.rpm  
b6ee8f8919df04406d00b4acf349cd6d  
corporate/3.0/x86\_64/mplayer-gui-1.0-0.pre3.14.14.C30mdk.x86\_64.rpm  
dd4f44dc8d0aa181b7ce3c5be006ef21 corporate/3.0/SRPMS/mplayer-1.0-0.pre3.14.14.C30mdk.src.rpm

---

To upgrade automatically use MandrivaUpdate 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-----

[ MDVSA-2008:045 ] – Updated MPlayer packages fix a few vulnerabilities

Version: GnuPG v1.4.8 (GNU/Linux)

iD8DBQFHtKhxmjqQ0CJFipgRAg7aAJ4sSkQEWvOkAcqIgrMTvSNELOcehwCgjJ48  
TjDGG+/w68g+rfx94Cc/Qq8=  
=rh3q  
-----END PGP SIGNATURE-----