

# [UNIX] MPlayer MMST and Real RTSP Multiple Heap Overflows

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-04/0134.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 04/25/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 25 Apr 2005 15:05:54 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

MPlayer MMST and Real RTSP Multiple Heap Overflows

---

## SUMMARY

Buffer Overflows were found in MpPayer MMST and Real RTSP allow attackers to execute arbitrary code.

## DETAILS

Vulnerable Systems:

\* MPlayer version 1.0pre6 and prior (including pre6a)

Immune Systems:

\* MPlayer version 1.0pre7

Two vulnerabilities were identified in MPlayer, which could be exploited by remote attackers to execute arbitrary commands. The first flaw is due to a heap overflow error in the MMST code when handling multiple stream IDs, which may be exploited via a malicious server to compromise a vulnerable system. The second vulnerability is due to a heap overflow error in the Real RTSP code when processing multiple lines (more than "MAX\_FIELDS" lines), which may be exploited via a malicious server to cause a denial of service and potentially compromise a vulnerable system.

Securiteam: [UNIX] MPlayer MMST and Real RTSP Multiple Heap Overflows

Vendor Status:

The vendor has released patch:

<[http://www.mplayerhq.hu/MPlayer/patches/rtsp\\_fix\\_20050415.diff](http://www.mplayerhq.hu/MPlayer/patches/rtsp_fix_20050415.diff)>

[http://www.mplayerhq.hu/MPlayer/patches/rtsp\\_fix\\_20050415.diff](http://www.mplayerhq.hu/MPlayer/patches/rtsp_fix_20050415.diff)

<[http://www.mplayerhq.hu/MPlayer/patches/mmst\\_fix\\_20050415.diff](http://www.mplayerhq.hu/MPlayer/patches/mmst_fix_20050415.diff)>

[http://www.mplayerhq.hu/MPlayer/patches/mmst\\_fix\\_20050415.diff](http://www.mplayerhq.hu/MPlayer/patches/mmst_fix_20050415.diff)

ADDITIONAL INFORMATION

The information has been provided by FrSIRT.

The original article can be found at:

<<http://www.frstirt.com/english/advisories/2005/0369>>

<http://www.frstirt.com/english/advisories/2005/0369>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.