

# [NT] Multiple Buffer Overruns RealOne / RealPlayer / RealOne Enterprise

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0073.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 11/22/02

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: 23 Nov 2002 00:40:28 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit [http://www.worldonline.co.za/services/work\\_ip.asp](http://www.worldonline.co.za/services/work_ip.asp)

-----

Multiple Buffer Overruns RealOne / RealPlayer / RealOne Enterprise

---

## SUMMARY

RealOne / RealPlayer are one of the most widely used products for internet media delivery. According to Real, there are currently around 115 million users worldwide. RealOne is the updated version of RealPlayer. Both suffer from multiple overrun issues.

## DETAILS

This advisory details three remotely exploitable overruns, two being heap based overflows and the other being a stack based overflow. On exploitation of these overruns any supplied code would execute in the security context of the logged on user.

1) By following a link to a SMIL file (Synchronized Multimedia Integration Language), RealPlayer will automatically download the file in an attempt to play its content. By supplying an overly long parameter within the SMIL file a heap overflow would occur in RealPlay.exe. According to Real, they have fixed the issue by fixing the player status code to handle the cases where there are large number of characters in the metadata of a SMIL file.

Securiteam: [NT] Multiple Buffer Overruns RealOne / RealPlayer / RealOne Enterprise

2) By supplying an overly long rtsp:// filename parameter, for example within a .m3u file, when a link was followed, Real again would download the file. When play is selected a heap overflow occurs in RealPlay.exe This has apparently been fixed by Real by improving the robustness of URL handling in this portion of the product.

3) Again, referring to number two if the 'victim' were to download the file with a large filename (whether it was on local/rtsp or an HTTP URL) Real Player would access violate when performing the following: If the user were to right click in Now Playing and select "Edit Clip info" or right click in "Now Playing" and "Select copy to my Library". In this particular instance a stack overflow would occur in RealPlayer.

Fix Information:

NGSSoftware alerted Real to these problems on the 1st November 2002. NGSSoftware highly recommend installing the patch found at <[http://service.real.com/help/faq/security/bufferoverrun\\_player.html](http://service.real.com/help/faq/security/bufferoverrun_player.html)> [http://service.real.com/help/faq/security/bufferoverrun\\_player.html](http://service.real.com/help/faq/security/bufferoverrun_player.html). Alternatively if you Open RealPlayer – Help – About Real Player, you will notice a Check For Updates feature. Select this.

In Real's own advisory they omit the fact that RealOne Enterprise Desktop is also vulnerable, but only to issues 2 & 3.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:mark@ngssoftware.com>> Mark Litchfield.

=====

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](mailto:list-unsubscribe@securiteam.com) In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.