

[UNIX] RealNetworks RealPlayer and Helix Player Invalid Chunk Size Heap Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00080.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 26 Mar 2006 16:06:22 +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>

RealNetworks RealPlayer and Helix Player Invalid Chunk Size Heap Overflow

SUMMARY

<<http://www.real.com/>> RealPlayer is an application for playing various media formats, developed by RealNetworks Inc.

Remote exploitation of a heap-based buffer overflow in RealNetwork Inc's RealPlayer could allow the execution of arbitrary code in the context of the currently logged in user.

DETAILS

Vulnerable Systems:

- * RealPlayer 10.5 (6.0.12.1040–1348)
- * RealPlayer 10
- * RealOne Player v2
- * RealOne Player v1
- * RealPlayer 8
- * Player 1.4 for Linux.
- * It is suspected that previous versions of RealPlayer and Helix Player are affected by this vulnerability.

[UNIX] RealNetworks RealPlayer and Helix Player Invalid Chunk Size Heap Overflow

The vulnerability specifically exists in the handling of the 'chunked' Transfer-Encoding method. This method breaks the file the server is sending up into 'chunks'. For each chunk, the server first sends the length of the chunk in hexadecimal, followed by the chunk data. This is repeated until there are no more chunks. The server then sends a chunk length of 0 indicating the end of the transfer.

There are multiple ways of triggering this vulnerability.

- * Sending a well-formed chunk header with a length of -1 (FFFFFFFF) followed by malicious data.
- * Sending a well-formed chunk header with a length specified which is less than the amount of data that will be sent, followed by malicious data.
- * Not sending a chunk header before sending malicious data.

Each of these cases result in a heap overflow. Depending on the versions used, certain of these cases will not cause exploitable issues. However, the last case appears to be reliable in triggering a crash.

Successful exploitation allows a remote attacker to execute arbitrary code with the privileges of the currently logged in user. In order to exploit this vulnerability, an attacker would need to entice a user to follow a link to a malicious server. Once the user visits a website under the control of an attacker, it is possible in a default install of RealPlayer to force a web-browser to use RealPlayer to connect to an arbitrary server, even when it is not the default application for handling those types, by the use of embedded object tags in a webpage. This may allow automated exploitation when the page is viewed.

As the client sends its version information as part of the request, it would be possible for an attacker to create a malicious server which uses the appropriate offsets and shellcode for each version and platform of the client.

Workaround:

Although there is no way to completely protect yourself from this vulnerability, aside from removing the RealPlayer software, the following actions may be taken to minimize the risk of automated exploitation.

Disable ActiveX controls and plugins, if not necessary for daily operations, using the following steps:

1. In IE, click on Tools and select Internet Options from the drop-down menu.
2. Click the Security tab and the Custom Level button.
3. Under ActiveX Controls and Plugins, then Run Activex Controls and Plugins, click the Disable radio button.

In general, exploitation requires that a targeted user be socially engineered into visiting a link to a server controlled by an attacker. As such, do not visit unknown/untrusted website and do not follow suspicious links.

[UNIX] RealNetworks RealPlayer and Helix Player Invalid Chunk Size Heap Overflow

When possible, run client software, especially applications such as IM clients, web browsers and e-mail clients, from regular user accounts with limited access to system resources. This may limit the immediate consequences of client-side vulnerabilities such as this.

Information from the vendor about this vulnerability is available at to following URL:

http://service.real.com/realplayer/security/03162006_player/en/
http://service.real.com/realplayer/security/03162006_player/en/

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2922>
CAN-2005-2922

Disclosure Timeline:

- * 08.09.05 Initial vendor notification
- * 09.09.05 Initial vendor response
- * 23.03.06 Public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense.

The original article can be found at:

<http://www.iddefense.com/intelligence/vulnerabilities/display.php?id=404>
<http://www.iddefense.com/intelligence/vulnerabilities/display.php?id=404>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

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.