

[NT] Directory Traversal In RealPlayer Allows Code Execution

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0038.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/16/04

To: list@securiteam.com

Date: 16 Feb 2004 11:50:35 +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>

Directory Traversal In RealPlayer Allows Code Execution

SUMMARY

<http://www.realnetworks.com/products/media_players.html> RealPlayer is a popular multimedia player developed by RealNetworks. One of its features are RMP files, RealJukebox Metadata Packages. These are XML formatted files which may contain e.g. playlists, references to skin files (*.rjs), and information about related web pages.

A directory traversal vulnerability exists in the player allowing an attacker to craft an RMP file which may upload files to arbitrary locations on the victim system. This could potentially lead to arbitrary code execution.

DETAILS

Vulnerable Systems:

- * RealOne Player and RealOne Player version 2 (Windows only)
- * RealPlayer 10 Beta (English only)
- * RealPlayer Enterprise
- * RealOne Enterprise Desktop

Securiteam: [NT] Directory Traversal In RealPlayer Allows Code Execution

RMP files are opened without confirmation if a web page uses JavaScript or an IFRAME tag to reference them. Therefore, it is possible to carry out an attack without further user interaction when the victim visits such a web page. The RMP file may contain references to a number of files as tags. The file extension determines how RealPlayer handles the file, ie. as audio, video, or a skin file. If the filename ends with ".rjs", it's assumed to be a skin file and downloaded to a location under the current user's profile folder. For RealOne Player the exact location is:

```
%USERPROFILE%\Application Data\Real\RealOne Player\skins\file.rjs
```

An attacker may use "..\" sequences in the file name to cause the skin file to be placed outside this folder. With a specially crafted filename, an attacker can place an arbitrarily named file with arbitrary contents anywhere on the victim system. Overwriting files isn't possible as RealPlayer asks for confirmation.

To run a desired program, an attacker can for instance place an HTML and EXE file on the victim system by using a single RMP file. The "related info" feature of RealPlayer can be used to automatically open the HTML file, which can then use JavaScript to launch the EXE file. A proof of concept RMP file was created to do this. Use of some unpatched Internet Explorer flaws are required for this exploit.

Another way is simply to place an EXE or other program in the current user's Startup folder to be launched during the next login. The attacker needn't know the login name; a relative path can be used because the default folder for skins is already under the user's profile folder.

Vendor Status:

Realnetworks were contacted on November 24, 2003 and have released an update to mitigate the vulnerability. The update can be found at http://service.real.com/help/faq/security/040123_player/EN/

ADDITIONAL INFORMATION

The information has been provided by <mailto:jouko@iki.fi> Jouko Pynnonen.

=====

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

=====
=====

Securiteam: [NT] Directory Traversal In RealPlayer Allows Code Execution

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.