

[NT] RealPlayer Arbitrary File Deletion Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0099.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/23/05

To: list@securiteam.com

Date: 23 Jan 2005 16:37:53 +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>

RealPlayer Arbitrary File Deletion Vulnerability

SUMMARY

A vulnerability has been discovered in RealPlayer that allows an attacker to delete arbitrary files from a users system through a specially crafted webpage with little user interaction.

DETAILS

Vulnerable Systems:

* RealPlayer version 10.5 (6.0.12.1040) and prior

RealPlayer supports a proprietary package delivery file type, aptly named Real Metadata Packages. These files contain an HTML style language which contains information and resource URLs for various packages and extensions to RealPlayer.

One of the supported tags within the RMP file type is the <FILENAME> tag. This is designed to point to a relative file which is to be downloaded. If the file which is to be downloaded already exists on the system, it will delete this file without warning.

Securiteam: [NT] RealPlayer Arbitrary File Deletion Vulnerability

It is also possible to insert directory traversal character sequences in the file name to break out of the download directory, and to point to any existing file on the system.

Before the the deletion takes place, RealPlayer ensures that the file extension is among those listed in the formats.ini file located at:
C:\Program Files\Real\RealPlayer\DataCache\Formats\formats.ini

It is possible to bypass this file extension check in the follow manner due to a lack in the file extension validation process:
<FILENAME>../../../../../../../../windows/system32/notepad.exe?.mp3</FILENAME>

Fix Information:

RealNetworks have released an update for the Real Meta Package file deletion vulnerability which can be downloaded from:
<http://service.real.com/help/faq/security/040928_player/EN/>
http://service.real.com/help/faq/security/040928_player/EN/

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nisr@nextgenss.com>>
NGSSoftware Insight Security Research.
The original article can be found at:
<<http://www.ngssoftware.com/advisories/real-02full.txt>>
<http://www.ngssoftware.com/advisories/real-02full.txt>

=====

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.