

[NT] RealPlayer 'ShowPreferences' Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0098.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/23/05

To: list@securiteam.com

Date: 23 Jan 2005 16:42:30 +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 'ShowPreferences' Buffer Overflow Vulnerability

SUMMARY

A vulnerability has been discovered in the RealPlayer ActiveX component that allows remote code execution when visiting a specially crafted webpage or when opening a specially crafted skin file.

DETAILS

Vulnerable Systems:

* RealPlayer version 10.5 (6.0.12.1040) and prior

The RealPlayer ActiveX component exports a function called HandleAction().

This function is designed to take a method or an action, and to execute it under a number of differing environments. This could be within a RealPlayer skin file or a webpage which is designed to interact with RealPlayer.

One of the 'actions' which HandleAction() will accept is 'ShowPreferences'. This method will accept two arguments, a category and the url of it's respective webpage.

Securiteam: [NT] RealPlayer 'ShowPreferences' Buffer Overflow Vulnerability

It has been discovered that passing overly long arguments to this method will result in an unbounded concatenation of the two arguments into a stack based buffer through an unchecked call to sprintf().

Fix Information:

RealNetworks have released an update for the ShowPreferences buffer overflow 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/)

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-01full.txt>](http://www.ngssoftware.com/advisories/real-01full.txt)

<http://www.ngssoftware.com/advisories/real-01full.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.