

[NT] Multiple Vulnerabilities in RealArcade (Integer Overflow, Files Deletion)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0094.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/22/05

To: list@securiteam.com

Date: 22 Feb 2005 15:10:18 +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>

Multiple Vulnerabilities in RealArcade (Integer Overflow, Files Deletion)

SUMMARY

<<http://www.realarcade.com/>> RealArcade is a software/portal developed by RealNetworks for downloading and buying arcade games.

RealArcade contains two security vulnerabilities, one is an integer overflow and the other is a file deletion vulnerability.

DETAILS

Vulnerable Systems:

* RealArcade version 1.2.0.994 and prior

Integer Overflow

The vulnerability lies in the handling of RGS files. Each RGS file is defined using an integer of a 32 bits that specifies the length of a GUID string and a name of a game to install.

When the user launches a RGS file he can choose if to continue installing or not.

The vulnerability allows to overwrite the return address of the vulnerable

Securiteam: [NT] Multiple Vulnerabilities in RealArcade (Integer Overflow, Files Deletion)

function which in turn can be used by an attacker to execute malicious code.

Arbitrary File Deletion

The mechanism of the RGP files allows an attacker to also delete any file on the victim's disk by simply using the content of RGP file containing a tag followed by a filename with a directory traversal path.

Example:

```
..
<GAMEID>950258D1-7ABD-4afc-8886-449B98CE8224</GAMEID>
<VERSION>1.0 Demo RGI</VERSION>
<TYPE>demo</TYPE>
<GENRE>Puzzle and Board</GENRE>

<!-- now we exploit the directory traversal bug -->

<FILENAME>../../windows/calc.exe</FILENAME>
..
```

The problem is caused by the fact that RealArcade will truncate the file (if it is present) to a 0 bytes size before it tries to write to it.

It appears that older versions could have been exploited using backslashes while recent versions can be only exploited using forward slashes.

ADDITIONAL INFORMATION

The information has been provided by <mailto:aluigi@autistici.org> Luigi Auriemma.

=====

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.