

[NEWS] RealPlayer Data Packet Stack Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0051.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/14/05

To: list@securiteam.com

Date: 14 Nov 2005 16:20:10 +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 Data Packet Stack Overflow

SUMMARY

Lack of proper length validation in RealPlayer's data packet handling allows attackers to cause the program to execute arbitrary code using a buffer overflow.

DETAILS

Vulnerable Systems:

- * RealPlayer version 10.5 (6.0.12.1040–1235) for Windows
- * RealPlayer version 10 for Windows
- * RealOne Player v2 for Windows
- * RealOne Player v1 for Windows
- * RealPlayer version 8 for Windows
- * RealPlayer Enterprise for Windows
- * RealPlayer 10 for Mac
- * RealPlayer 10 (10.0.0 – 5) for Linux
- * Helix Player (10.0.0 – 5) for Linux

This specific flaw exists in the first data packet contained in a Real Media file. By specially crafting a malformed .rm movie file, a direct stack overwrite is triggered, and reliable code execution is then possible.

Securiteam: [NEWS] RealPlayer Data Packet Stack Overflow

The vulnerability is triggered by setting the application specific length field of the [data packet + 1] to 0x80 – 0xFF this will cause a stack overflow. The value is sign–extended and passed as the length to memcpy.

Vendor Status:

The vendor has issued a patch:

<http://service.real.com/help/faq/security/051110_player/EN/>

http://service.real.com/help/faq/security/051110_player/EN/

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2629>>

CAN-2005-2629

ADDITIONAL INFORMATION

The information has been provided by <mailto:Advisories@eeye.com> Eeye.

The vendor advisory can be found at:

<http://service.real.com/help/faq/security/051110_player/EN/>

http://service.real.com/help/faq/security/051110_player/EN/

=====

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.