

Security Update For RealPlayer

Updated October 19th, 2007

RealNetworks, Inc. has addressed a recently discovered security vulnerability that affects an ActiveX control installed by RealPlayer while running in an embedded environment within Microsoft Corp.'s Internet Explorer (IE) browser. The vulnerability can be exploited to run arbitrary code by causing a user to visit a specially crafted web page.

Impacted Products and Versions:

This affects RealPlayer v10.5 and v11. The currently available enterprise build (6.0.11.x) is unaffected as the implementation of the ActiveX control for RealPlayer Enterprise only uses a small subset of the consumer player's authoring control and avoids importing files to the library.

Workaround / Resolution:

Some mitigating strategies that you can put in place until patches are available as recommended by [Symantec](#):

- Set the kill bit on the Class identifier (CLSID) FDC7A535-4070-4B92-A0EA-D9994BCC0DC5, (see instructions here: <http://support.microsoft.com/kb/240797>)
- Ensure that all Microsoft Internet Explorer clients are configured to prompt before executing Active Scripting. If Active Scripting is not required it should be disabled completely.
- Ensure that all Microsoft Outlook and Outlook Express clients are configured to either display all incoming email in plain text format, or that HTML email messages are opened in the Restricted sites security zone.
- Ensure that antivirus software is up to date.
- As most vulnerabilities of this nature rely on JavaScript to carry out exploitation, customers are advised to disable JavaScript whenever possible.
- Always execute Web browser software as a user with minimal system privileges.

Resolution:

RealPlayer 10.5 and RealPlayer 11 Beta users should install the following [patch](#) to address this security vulnerability. For more information, go to the [RealPlayer security site](#).

Acknowledgements:

RealNetworks would like to thank Will Dormann of CERT and anonymous researchers working on bringing this exploit to our attention as well as those who subsequently worked with RealNetworks to correct the vulnerabilities.

Warranty:

RealNetworks Inc. endeavors to provide you with the highest quality products and services, but cannot guarantee, and does not warrant, that the operation of any RealNetworks product will

be error-free, uninterrupted or secure. Please see your original license agreement for details of our limited warranty or warranty disclaimer.