

Security Update For RealPlayer Enterprise

Updated October 25th, 2007

RealNetworks, Inc. has addressed a recently discovered security vulnerabilities that offered the potential for specific files types to cause a heap overflow on a customer's machine. RealNetworks takes all security vulnerabilities extremely seriously and provide this information as an aid for users to avoid any potential vulnerabilities.

The specific exploits were:

- Vulnerability 1:

The identified vulnerability is a malicious mp3 file which could cause a heap overflow in the RealPlayer. CVE-2007-5080.

- Vulnerability 2:

The identified vulnerability is a malicious rm file which could cause a heap overflow in the RealPlayer. CVE-2007-5081.

- Vulnerability 3:

The identified vulnerability is a malicious SMIL file which could cause a buffer overflow in the RealPlayer. CVE-2007-3410

- Vulnerability 4:

The identified vulnerability is a malicious swf file (flash media) which could cause a heap overflow on a customer's machine. CVE-2007-2263.

- Vulnerability 5:

The identified vulnerability is a malicious ram file which could cause a heap overflow in the RealPlayer. CVE-2007-2264

Impacted Products and Versions:

This affects all versions of RealPlayer Enterprise prior to v1.11 (standalone and as configured by the RealPlayer Enterprise Manager). To identify which build number is currently in use, click on Help > About RealPlayer. Ensure the Enterprise Player build number is greater than or equal to 6.0.11.2160 to avoid being affected. (This build number is ONLY relevant to the Enterprise build)

Workaround / Resolution:

To ensure that your Player is protected, we recommend installing the latest version of RealPlayer Enterprise Manager and then create a new Enterprise Player or to download the Enterprise Standalone player from your company's Product and Account Maintenance (PAM) site.

UPDATES

RealPlayer Enterprise Solution:

Please [click here](#) to get the updated RealPlayer Enterprise Manager. Your PAM site will contain a complete / updated copy of RPE.

Acknowledgements:

RealNetworks would like to acknowledge John Heasman of [NGS Software](#), [Piotr Bania](#), and anonymous researchers working with [TippingPoint](#) and the [Zero Day Initiative](#) for bringing these exploits 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.