

Security Update For RealPlayer Enterprise

Updated January 26, 2010

RealNetworks is making available product upgrades that contain security bug fixes.

RealNetworks, Inc. has addressed recently discovered security vulnerabilities. RealNetworks takes all security vulnerabilities extremely seriously and provides this information as an aid for users to avoid any potential vulnerability.

Details of potential vulnerabilities:

CVE-2009-4247: RealPlayer ASM RuleBook Array Overflow

CVE-2009-4257: RealPlayer SMIL Parsing Heap Overflow Vulnerability

Impacted Products and Versions:

RealPlayer Enterprise 2.1.1 - version 6.0.12.1798

RealPlayer Enterprise 1.14 - version 6.0.11.2651

Resolution:

Upgrade to RealPlayer Enterprise 2.1.2 - version 6.0.12.1810

Acknowledgements:

RealNetworks would like to acknowledge anonymous researchers working with [iDEFENSE Labs](#), John Rambo and anonymous researchers working with [TippingPoint](#) 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.