

Security Update For RealPlayer Enterprise

Updated August 16, 2011

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 provide this information as an aid for users to avoid any potential vulnerabilities.

Impacted Products and Versions:

The currently available enterprise build 6.0.12.1836 (software version 2.1.6) addresses all vulnerabilities listed in this document. The impacted version of RealPlayer Enterprise can be found with each announcement under Affected Software.

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 6.0.12.1836 to avoid being affected. (This build number is ONLY relevant to the Enterprise build)

RealPlayer Enterprise uses a subset of the consumer player's features and is not affected by all vulnerabilities in this document. The vulnerabilities that do not affect RealPlayer Enterprise are included at the end of this document as a courtesy to our customers.

Workaround / Resolution:

To ensure that your Player is protected, we recommend installing the latest version of RealPlayer Enterprise.

Details for Potential Vulnerabilities:

CVE Descriptions

CVE-2011-2946

RealPlayer ActiveX Remote Code Execution Vulnerability

Affected software: Windows RealPlayer 14.0.5 and prior.

Credit to getB33r working with [iDefense Labs](#) for reporting this issue.

CVE-2011-2948

RealPlayer SWF DefineFont Remote Code Execution Vulnerability
Affected software: Windows RealPlayer 14.0.5 and prior; RealPlayer Enterprise 2.1.5 and prior; Mac RealPlayer 12.0.0.1569 and prior.
Credit to Luigi Auriemma working with [TippingPoint's Zero Day Initiative](#) for reporting this issue.

CVE-2011-2949

RealPlayer MP3 ID3 tags Remote Code Execution Vulnerability
Affected software: Windows RealPlayer 14.0.5 and prior; RealPlayer Enterprise 2.1.5 and prior.
Credit to Sean de Regge working with [TippingPoint's Zero Day Initiative](#) for reporting this issue.

CVE-2011-2952

RealPlayer Dialog Box Use After Free Vulnerability
Affected software: Windows RealPlayer 14.0.5 and prior; RealPlayer Enterprise 2.1.5 and prior.
Credit to Krystian Kloskowski (h07) via [Secunia Research](#) for reporting this issue.

CVE-2011-2953

RealPlayer ActiveX Browser Plugin Out of Bounds Vulnerability.
Affected software: Windows RealPlayer 14.0.5 and prior.
Credit to [Luigi Auriemma](#) for reporting this issue.

CVE-2011-2955

RealPlayer Embedded Modal Dialog Use After Free Vulnerability
Affected software: Windows RealPlayer 14.0.5 and prior; RealPlayer Enterprise 2.1.5 and prior.
Credit to [Luigi Auriemma](#) for reporting this issue.

RealPlayer Enterprise is not affected by the following Vulnerabilities:**CVE-2011-2945**

RealPlayer SIPR Heap Buffer Overflow Vulnerability
Affected software: Windows RealPlayer 14.0.5 and prior.
Credit to Omair, [iDefense Labs](#) for reporting this issue.

CVE-2011-2947

RealPlayer Cross-Zone Scripting Remote Code Execution Vulnerability

Affected software: Windows RealPlayer 14.0.5 and prior; RealPlayer Enterprise 2.1.5 and prior; Mac RealPlayer 12.0.0.1569 and prior.
Credit to Martin Bartek working with [TippingPoint's Zero Day Initiative](#) for reporting this issue.

CVE-2011-2950

RealPlayer QCP Parsing Remote Code Execution Vulnerability
Affected software: Windows RealPlayer 14.0.5 and prior.
Credit to Sean de Regge working with [TippingPoint's Zero Day Initiative](#) for reporting this issue.

CVE-2011-2951

RealPlayer Advanced Audio Coding Element Remote Code Execution Vulnerability
Affected software: Windows RealPlayer 14.0.5 and prior; Mac RealPlayer 12.0.0.1569 and prior.
Credit to Donato Ferrante and Andrzej Dyjak working with [TippingPoint's Zero Day Initiative](#) for reporting this issue.

CVE-2011-2954

RealPlayer Embedded AutoUpdate Use After Free Vulnerability
Affected software: Windows RealPlayer 14.0.5 and prior.
Credit to [Luigi Auriemma](#) for reporting this issue.

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.