



# CVE-2007-2263

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2007-2263
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-10-31 17:46:00 UTC
<b>Updated</b>	2026-04-23 00:35:47 UTC
<b>Description</b>	Heap-based buffer overflow in RealNetworks RealPlayer 10.0, 10.1, and possibly 10.5, RealOne Player, and RealPlayer Er

## Risk And Classification

**Primary CVSS:** v2.0 9.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:C/I:C/A:C

**Problem Types:** CWE-119 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:N/C:C/I:C/A:C

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Realnetworks	Realone Player	All	All	mac	en

Application	<a href="#">Realnetworks</a>	<a href="#">Realone Player</a>	2.0	All	windows	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.0	All	windows	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.0	10.0.0.305	mac	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.0	10.0.0.331	mac	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.0	10.0.0.352	mac	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.0	10.0.5	linux	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.0	10.0.6	linux	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.0	10.0.7	linux	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.0	10.0.8	linux	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.0	10.0.9	linux	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.1	10.0.0.396	mac	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.1	10.0.0.412	mac	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.5	6.0.12.1040	windows	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.5	6.0.12.1578	windows	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.5	6.0.12.1698	windows	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.5	6.0.12.1741	windows	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer Enterprise</a>	All	All	windows	en

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

#### References

##### Reference

RealNetworks RealPlayer File Parsing Routines Multiple Vulnerabilities

[osvdb.org/38344](https://osvdb.org/38344)

RealPlayer/RealOne/HelixPlayer Multiple Buffer Overflows - Advisories - Secunia

[VIM] RealPlayer Updates of October 25, 2007

RealNetworks RealPlayer SWF File Processing Remote Code Execution Vulnerability

Repository / Oval Repository

SecurityTracker.com Archives - RealPlayer Buffer Overflows in Processing MP3, RM, SWF, RAM, and PLS Files Lets Remote Users Execute

Webmail - OVH

IBM X-Force Exchange

RealPlayer and StarSearch by Real Official Homepage — Real.com

Zero Day Initiative

SecurityFocus

CVE Program record



### Vendor Comments And Credit

Organization	Published	Contributor	Statement
--------------	-----------	-------------	-----------

Red Hat	2007-11-01	Mark J Cox	This issue was fixed in RealPlayer for Red Hat Enterprise Linux 3 Extras, 4 Extras, 5 Supplemer
---------	------------	------------	---



There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)