



# CVE-2005-2629

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2005-2629
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-11-18 23:03:00 UTC
<b>Updated</b>	2025-04-03 01:03:51 UTC
<b>Description</b>	Integer overflow in RealNetworks RealPlayer 8, 10, and 10.5, RealOne Player 1 and 2, and Helix Player 10.0.0 allows remote

## Risk And Classification

**Primary CVSS:** v2.0 5.1 from nvd@nist.gov

AV:N/AC:H/Au:N/C:P/I:P/A:P

**Problem Types:** NVD-CWE-Other | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:H/Au:N/C:P/I:P/A:P

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Realnetworks	Helix Player	1.0	All	linux	All

Application	<a href="#">Realnetworks</a>	<a href="#">Helix Player</a>	1.0.1	All	linux	All
Application	<a href="#">Realnetworks</a>	<a href="#">Helix Player</a>	1.0.2	All	linux	All
Application	<a href="#">Realnetworks</a>	<a href="#">Helix Player</a>	1.0.3	All	linux	All
Application	<a href="#">Realnetworks</a>	<a href="#">Helix Player</a>	1.0.4	All	linux	All
Application	<a href="#">Realnetworks</a>	<a href="#">Helix Player</a>	1.0.5	All	linux	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realone Player</a>	1.0	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realone Player</a>	2.0	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	All	All	enterprise	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.0	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.0	All	linux	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.0	All	mac_os_x	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.5	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.5_6.0.12.1040	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.5_6.0.12.1053	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.5_6.0.12.1056	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.5_6.0.12.1059	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.5_6.0.12.1069	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.5_6.0.12.1235	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	8.0	All	win32	All

### Vendor Declared Affected Products

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

### References

#### Reference

- SecurityTracker.com Archives - RealPlayer Enterprise Buffer Overflows in Processing .rm Files and Skin Files Lets Remote Users Execute Arbitrary Code
- SecurityTracker.com Archives - Helix Player Buffer Overflows in Processing .rm Files and Skin Files Lets Remote Users Execute Arbitrary Code
- Repository / Oval Repository
- '[EEYEB-20050510] - RealPlayer Data Packet Stack Overflow' - MARC
- Customer Support - Real Security Updates
- Secunia - Advisories - Debian update for helix-player
- Debian -- Security Information -- DSA-915-1 helix-player
- RealPlayer Data Packet Stack Overflow - CXSecurity.com
- IBM X-Force Exchange
- RealNetworks RealOne Player/RealPlayer RM File Remote Stack Based Buffer Overflow Vulnerability
- Secunia - Advisories - RealPlayer/RealOne/HelixPlayer ".rm" and ".ria" File Handling Buffer Overflow

Secunia - Advisories - RealPlayer/RealOne/RealPlayer .rm and .rjs File Handling Buffer Overflow

SecurityTracker.com Archives - RealPlayer/RealOne Player Buffer Overflows in Processing .rm Files and Skin Files Lets Remote Users Execu

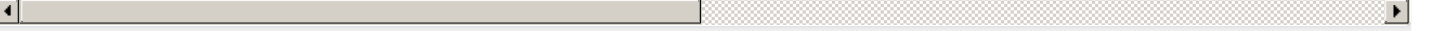
Secunia - Advisories - SUSE Updates for Multiple Packages

Network Security, Vulnerability Assessment, Intrusion Prevention

RealNetworks RealOne Player/RealPlayer RM File Remote Stack Based Buffer Overflow Vulnerability

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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

**CVE.report and Source URL Uptime Status** [status.cve.report](#)