



# CVE-2005-2922

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

## Summary

<b>CVE</b>	CVE-2005-2922
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-12-31 05:00:00 UTC
<b>Updated</b>	2025-04-03 01:03:51 UTC
<b>Description</b>	Heap-based buffer overflow in the embedded player in multiple RealNetworks products and versions including RealPlayer 1

## 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	Helix Player	10.0	All	linux	All

Application	Realnetworks	Helix Player	10.0.1	All	linux	All
Application	Realnetworks	Helix Player	10.0.2	All	linux	All
Application	Realnetworks	Helix Player	10.0.3	All	linux	All
Application	Realnetworks	Helix Player	10.0.4	All	linux	All
Application	Realnetworks	Helix Player	10.0.5	All	linux	All
Application	Realnetworks	Helix Player	10.0.6	All	linux	All
Application	Realnetworks	Realone Player	All	All	All	All
Application	Realnetworks	Realone Player	0.288	All	mac_os_x	All
Application	Realnetworks	Realone Player	0.297	All	mac_os_x	All
Application	Realnetworks	Realone Player	1.0	All	All	All
Application	Realnetworks	Realone Player	2.0	All	All	All
Application	Realnetworks	Realplayer	All	All	enterprise	All
Application	Realnetworks	Realplayer	10.0	All	All	All
Application	Realnetworks	Realplayer	10.0.0.305	All	mac_os	All
Application	Realnetworks	Realplayer	10.0.0.331	All	mac_os	All
Application	Realnetworks	Realplayer	10.0.1	All	linux	All
Application	Realnetworks	Realplayer	10.0.2	All	linux	All
Application	Realnetworks	Realplayer	10.0.3	All	linux	All
Application	Realnetworks	Realplayer	10.0.4	All	linux	All
Application	Realnetworks	Realplayer	10.0.5	All	linux	All
Application	Realnetworks	Realplayer	10.0.6	All	linux	All
Application	Realnetworks	Realplayer	10.5	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1040	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1053	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1056	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1059	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1069	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1235	All	All	All
Application	Realnetworks	Realplayer	8.0	All	win32	All
Application	Realnetworks	Rhapsody	3.0	All	All	All
Application	Realnetworks	Rhapsody	3.0_build_0.815	All	All	All

#### Vendor Declared Affected Products

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

#### References

REFERENCES

Reference	Source
Repository / Oval Repository	af854a3a-2
rhn.redhat.com   Red Hat Support	af854a3a-2
About Secunia Research   Flexera	af854a3a-2
SUSE update for RealPlayer - Advisories - Secunia	af854a3a-2
Webmail - OVH	af854a3a-2
US-CERT Vulnerability Note VU#172489	af854a3a-2
RealNetworks Multiple Products Multiple Buffer Overflow Vulnerabilities	af854a3a-2
Security Announcement	af854a3a-2
404 Not Found	af854a3a-2
IBM X-Force Exchange	af854a3a-2
Support	af854a3a-2
SecurityTracker.com Archives - RealPlayer Heap Overflow in Embedded Player May Let Remote Users Execute Arbitrary Code	af854a3a-2
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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)