



CVE-2005-0611

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

Summary

CVE	CVE-2005-0611
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-02 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Heap-based buffer overflow in RealNetworks RealPlayer 10.5 (6.0.12.1056 and earlier), 10, 8, and RealOne Player V2 and

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	All	All	All	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	10.5	All	All	All
Application	Realnetworks	Realplayer	8.0	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source	Link
Customer Support - Real Security Updates	af854a3a-2127-422b-91ae-364da2661108	sc
'[VulnWatch] RealOne Player / Real .WAV Heap Overflow File Format Vulnerability' - MARC	af854a3a-2127-422b-91ae-364da2661108	m
'RealOne Player / Real .WAV Heap Overflow File Format Vulnerability' - MARC	af854a3a-2127-422b-91ae-364da2661108	m
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	ov
rhn.redhat.com Red Hat Support	af854a3a-2127-422b-91ae-364da2661108	w
rhn.redhat.com Red Hat Support	af854a3a-2127-422b-91ae-364da2661108	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	m

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](#)