



# CVE-2009-4244

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

## Summary

<b>CVE</b>	CVE-2009-4244
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2010-01-25 19:30:01 UTC
<b>Updated</b>	2026-04-29 01:13:23 UTC
<b>Description</b>	Heap-based buffer overflow in RealNetworks RealPlayer 10; RealPlayer 10.5 6.0.12.1040 through 6.0.12.1741; RealPlayer

## 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
Operating System	Microsoft	Windows	All	All	All	All

Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.0	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.5	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	11.0	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	11.0.1	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	11.0.2	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	11.0.3	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	11.0.4	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	11.0.5	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer Enterprise</a>	All	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer Sp</a>	1.0.0	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer Sp</a>	1.0.1	All	All	All

#### Vendor Declared Affected Products

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

#### References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	<a href="#">af854a3a-2127-422b-91ae-364da26</a>
SecurityFocus	<a href="#">af854a3a-2127-422b-91ae-364da26</a>
RealPlayer and StarSearch by Real Official Homepage — Real.com	<a href="#">af854a3a-2127-422b-91ae-364da26</a>
Multiple RealNetworks Products Multiple Remote Vulnerabilities	<a href="#">af854a3a-2127-422b-91ae-364da26</a>
Zero Day Initiative	<a href="#">af854a3a-2127-422b-91ae-364da26</a>
IBM X-Force Exchange	<a href="#">af854a3a-2127-422b-91ae-364da26</a>
SecurityTracker.com Archives - RealPlayer Buffer Overflows Let Remote Users Execute Arbitrary Code	<a href="#">af854a3a-2127-422b-91ae-364da26</a>
RealPlayer Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	<a href="#">af854a3a-2127-422b-91ae-364da26</a>
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.

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](https://cve.report/api)

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