



# CVE-2006-0323

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

## Summary

<b>CVE</b>	CVE-2006-0323
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-03-23 23:06:00 UTC
<b>Updated</b>	2025-04-03 01:03:51 UTC
<b>Description</b>	Buffer overflow in swfformat.dll in multiple RealNetworks products and versions including RealPlayer 10.x, RealOne Player,

## 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

**EPSS:** 0.684670000 probability, percentile 0.986180000 (date 2026-04-19)

**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	<a href="#">Realnetworks</a>	<a href="#">Helix Player</a>	All	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realone Player</a>	All	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.0	gold	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.0.6	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Realplayer</a>	10.5	All	All	All
Application	<a href="#">Realnetworks</a>	<a href="#">Rhapsody</a>	3	All	All	All

### Vendor Declared Affected Products

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

### References

#### Reference

- [Red Hat update for realplayer - Advisories - Secunia](#)
- [Gentoo Linux Documentation -- RealPlayer: Buffer overflow vulnerability](#)
- [SecurityTracker.com Archives - RealPlayer Buffer Overflow in Processing SWF Flash Files Lets Remote Cause Arbitrary Code to Be Executed](#)
- [About Secunia Research | Flexera](#)
- [US-CERT Vulnerability Note VU#231028](#)
- [SUSE update for RealPlayer - Advisories - Secunia](#)
- [SecurityReason](#)
- [Gentoo update for realplayer - Advisories - Secunia](#)
- [Webmail - OVH](#)
- [RealNetworks Multiple Products Multiple Buffer Overflow Vulnerabilities](#)
- [Security Announcement](#)
- [404 Not Found](#)
- [IBM X-Force Exchange](#)
- [Support](#)
- [SecurityFocus](#)
- [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.

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

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