



CVE-2013-4973

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2013-4973
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-08-27 03:34:35 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Stack-based buffer overflow in RealNetworks RealPlayer before 16.0.3.51, and RealPlayer SP 1.0 through 1.1.5, allows re

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	Realplayer	10.0	All	All	All

Application	Realnetworks	Realplayer	10.5	All	All	All
Application	Realnetworks	Realplayer	11.0	All	All	All
Application	Realnetworks	Realplayer	11.0.1	All	All	All
Application	Realnetworks	Realplayer	11.0.2	All	All	All
Application	Realnetworks	Realplayer	11.0.2.1744	All	All	All
Application	Realnetworks	Realplayer	11.0.2.2315	All	All	All
Application	Realnetworks	Realplayer	11.0.3	All	All	All
Application	Realnetworks	Realplayer	11.0.4	All	All	All
Application	Realnetworks	Realplayer	11.0.5	All	All	All
Application	Realnetworks	Realplayer	11.1	All	All	All
Application	Realnetworks	Realplayer	11.1.3	All	All	All
Application	Realnetworks	Realplayer	11_build_6.0.14.748	All	All	All
Application	Realnetworks	Realplayer	12.0.0.1444	All	All	All
Application	Realnetworks	Realplayer	12.0.0.1548	All	All	All
Application	Realnetworks	Realplayer	14.0.0	All	All	All
Application	Realnetworks	Realplayer	14.0.1	All	All	All
Application	Realnetworks	Realplayer	14.0.1.609	All	All	All
Application	Realnetworks	Realplayer	14.0.2	All	All	All
Application	Realnetworks	Realplayer	14.0.3	All	All	All
Application	Realnetworks	Realplayer	14.0.4	All	All	All
Application	Realnetworks	Realplayer	14.0.5	All	All	All
Application	Realnetworks	Realplayer	15.0.0	All	All	All
Application	Realnetworks	Realplayer	15.0.4	All	All	All
Application	Realnetworks	Realplayer	15.0.4.43	All	All	All
Application	Realnetworks	Realplayer	15.0.5.109	All	All	All
Application	Realnetworks	Realplayer	15.0.6.14	All	All	All
Application	Realnetworks	Realplayer	15.02.71	All	All	All
Application	Realnetworks	Realplayer	16.0.0	All	All	All
Application	Realnetworks	Realplayer	16.0.0.282	All	All	All
Application	Realnetworks	Realplayer	16.0.1.18	All	All	All
Application	Realnetworks	Realplayer	All	All	All	All
Application	Realnetworks	Realplayer Sp	1.0.0	All	All	All
Application	Realnetworks	Realplayer Sp	1.0.1	All	All	All
Application	Realnetworks	Realplayer Sp	1.0.2	All	All	All
Application	Realnetworks	Realplayer Sp	1.0.5	All	All	All
Application	Realnetworks	Realplayer Sp	1.1	All	All	All

Application	Realnetworks	Realplayer Sp	1.1.1	All	All	All
Application	Realnetworks	Realplayer Sp	1.1.2	All	All	All
Application	Realnetworks	Realplayer Sp	1.1.3	All	All	All
Application	Realnetworks	Realplayer Sp	1.1.4	All	All	All
Application	Realnetworks	Realplayer Sp	1.1.5	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Vulnerability Note VU#246524 - Real Media Player filename handler stack buffer overflow vulnerability	af854a3a-2127-422b-91ae-364da26
August 2013	af854a3a-2127-422b-91ae-364da26
Real Networks RealPlayer CVE-2013-4973 Stack Based Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da26
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](#) 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](#)