



CVE-2011-0694

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

Summary

CVE	CVE-2011-0694
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-02-21 18:00:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	RealNetworks RealPlayer 11.0 through 11.1, SP 1.0 through 1.1.5, and 14.0.0 through 14.0.1, and Enterprise 2.0 through 2

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: NVD-CWE-Other | 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	11.0	All	All	All

Application	Realnetworks	Realplayer	11.1	All	All	All
Application	Realnetworks	Realplayer	14.0.0	All	All	All
Application	Realnetworks	Realplayer	14.0.1	All	All	All
Application	Realnetworks	Realplayer	2.0	All	enterprise	All
Application	Realnetworks	Realplayer	2.1	All	enterprise	All
Application	Realnetworks	Realplayer	2.1.2	All	enterprise	All
Application	Realnetworks	Realplayer	2.1.3	All	enterprise	All
Application	Realnetworks	Realplayer	2.1.4	All	enterprise	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	
Zero Day Initiative					af854a3a-2127-422b-91ae-3	
Feb. 2011 Update					af854a3a-2127-422b-91ae-3	
RealPlayer Predictable Temporary Filename Lets Remote Users Execute Arbitrary Code - SecurityTracker					af854a3a-2127-422b-91ae-3	
RealPlayer Predictable Temporary Filename Code Execution Vulnerability - Secunia.com					af854a3a-2127-422b-91ae-3	
docs.real.com/docs/security/SecurityUpdate020811RPE.pdf					af854a3a-2127-422b-91ae-3	
osvdb.org/70849					af854a3a-2127-422b-91ae-3	
RealNetworks Real Player Predictable Temporary File Remote Code Execution Vulnerability - CXSecurity.com					af854a3a-2127-422b-91ae-3	
SecurityFocus					af854a3a-2127-422b-91ae-3	
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](#)