

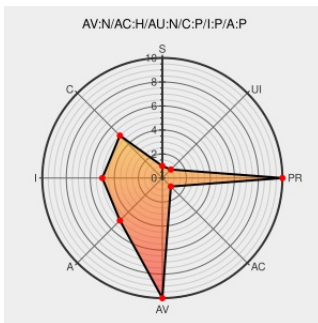


CVE-2004-1481

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 08/11/2021 02:19:00 PM UTC

CVE-2004-1481

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Helix Player](#) from [Realnetworks](#) contain the following vulnerability:

Integer overflow in pnen3260.dll in RealPlayer 8 through 10.5 (6.0.12.1040) and earlier, and RealOne Player 1 or 2 on Windows or Mac OS, allows remote attackers to execute arbitrary code via a SMIL file and a .rm movie file with a large length field for the data chunk, which leads to a heap-based buffer overflow.

CVE-2004-1481 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5.1 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

HIGH

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

'EEYE: RealPlayer pnen3260.dll Heap Overflow' - MARC

[Mailing List](#)
[Third Party Advisory](#)
[marc.info](#)
[text/html](#)

[BUGTRAQ 20041001 EEYE: RealPlayer pnen3260.dll Heap Overflow](#)

RealNetworks RealOne Player And RealPlayer P Nen3260.DLL Remote Integer Overflow Vulnerability

[Patch](#)
[Third Party Advisory](#)
[VDB Entry](#)
[cve.report \(archive\)](#)
[text/html](#)

[BID 11309](#)

Secunia - Advisories - RealOne Player / RealPlayer / Helix Player Multiple Vulnerabilities

[Third Party Advisory](#)
[web.archive.org](#)
[text/html](#)

[SECUNIA 12672](#)

IBM X-Force Exchange

Third Party Advisory

VDB Entry

exchange.xforce.ibmcloud.com

text/html

XF realplayer-rm-code-execution(17549)

Customer Support - Real Security Updates

Broken Link

web.archive.org

text/html

Inactive Link

Not Archived

CONFIRM

www.service.real.com/help/faq/security/040928_player/EN/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Realnetworks	Helix Player	1.0	All	All	All
Application	Realnetworks	Helix Player	1.0	All	All	All
Application	Realnetworks	Realone Player	1.0	All	All	All
Application	Realnetworks	Realone Player	2.0	All	All	All
Application	Realnetworks	Realone Player	9.0.0.288	All	All	All
Application	Realnetworks	Realone Player	9.0.0.288	All	All	All
Application	Realnetworks	Realone Player	9.0.0.297	All	All	All
Application	Realnetworks	Realone Player	9.0.0.297	All	All	All
Application	Realnetworks	Realone Player	1.0	All	All	All
Application	Realnetworks	Realone Player	2.0	All	All	All
Application	Realnetworks	Realone Player	9.0.0.288	All	All	All
Application	Realnetworks	Realone Player	9.0.0.297	All	All	All
Application	Realnetworks	Realplayer	-	All	All	All
Application	Realnetworks	Realplayer	10.0	All	All	All
Application	Realnetworks	Realplayer	10.0	All	All	All
Application	Realnetworks	Realplayer	10.0	All	All	de
Application	Realnetworks	Realplayer	10.0	All	All	en
Application	Realnetworks	Realplayer	10.0	All	All	ja
Application	Realnetworks	Realplayer	10.0	beta	All	All
Application	Realnetworks	Realplayer	10.0	beta	All	All
Application	Realnetworks	Realplayer	10.0_6.0.12.690	All	All	All
Application	Realnetworks	Realplayer	10.5	All	All	All
Application	Realnetworks	Realplayer	10.5 6.0.12.1016	beta	All	All

Application	Realnetworks	Realplayer	10.5_6.0.12.1040	All	All	All
Application	Realnetworks	Realplayer	8.0	All	All	All
Application	Realnetworks	Realplayer	8.0	All	All	All
Application	Realnetworks	Realplayer	8.0	All	All	All
Application	Realnetworks	Realplayer	-	All	All	All
Application	Realnetworks	Realplayer	10.0	All	All	All
Application	Realnetworks	Realplayer	10.0	All	All	All
Application	Realnetworks	Realplayer	10.0	All	All	de
Application	Realnetworks	Realplayer	10.0	All	All	en
Application	Realnetworks	Realplayer	10.0	All	All	ja
Application	Realnetworks	Realplayer	10.0	beta	All	All
Application	Realnetworks	Realplayer	10.0	beta	All	All
Application	Realnetworks	Realplayer	10.0_6.0.12.690	All	All	All
Application	Realnetworks	Realplayer	10.5	All	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1016	beta	All	All
Application	Realnetworks	Realplayer	10.5_6.0.12.1040	All	All	All
Application	Realnetworks	Realplayer	8.0	All	All	All
Application	Realnetworks	Realplayer	8.0	All	All	All
Application	Realnetworks	Realplayer	8.0	All	All	All
cpe:2.3:a:realnetworks:helix_player:1.0:*:*:*:*:linux:*:*:						
cpe:2.3:a:realnetworks:helix_player:1.0:*:*:*:*:linux:*:*:						
cpe:2.3:a:realnetworks:realone_player:1.0:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realone_player:2.0:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realone_player:9.0.0.288:*:*:*:*:macos:*:*:						
cpe:2.3:a:realnetworks:realone_player:9.0.0.288:*:*:*:*:mac_os_x:*:*:						
cpe:2.3:a:realnetworks:realone_player:9.0.0.297:*:*:*:*:macos:*:*:						
cpe:2.3:a:realnetworks:realone_player:9.0.0.297:*:*:*:*:mac_os_x:*:*:						
cpe:2.3:a:realnetworks:realone_player:1.0:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realone_player:2.0:*:*:*:*:*:						
cpe:2.3:a:realnetworks:realone_player:9.0.0.288:*:*:*:*:mac_os_x:*:*:						
cpe:2.3:a:realnetworks:realone_player:9.0.0.297:*:*:*:*:mac_os_x:*:*:						
cpe:2.3:a:realnetworks:realplayer:-:*:*:*:*:enterprise:*:*:						

cpe:2.3:a:realnetworks:realplayer:10.0:****:****:
cpe:2.3:a:realnetworks:realplayer:10.0:****:linux:****:
cpe:2.3:a:realnetworks:realplayer:10.0:****:de:****:
cpe:2.3:a:realnetworks:realplayer:10.0:****:en:****:
cpe:2.3:a:realnetworks:realplayer:10.0:****:ja:****:
cpe:2.3:a:realnetworks:realplayer:10.0:beta:****:****:
cpe:2.3:a:realnetworks:realplayer:10.0:beta:****:mac_os_x:****:
cpe:2.3:a:realnetworks:realplayer:10.0_6.0.12.690:****:****:
cpe:2.3:a:realnetworks:realplayer:10.5:****:****:
cpe:2.3:a:realnetworks:realplayer:10.5_6.0.12.1016:beta:****:****:
cpe:2.3:a:realnetworks:realplayer:10.5_6.0.12.1040:****:****:
cpe:2.3:a:realnetworks:realplayer:8.0:****:****:
cpe:2.3:a:realnetworks:realplayer:8.0:****:mac_os_x:****:
cpe:2.3:a:realnetworks:realplayer:8.0:****:unix:****:
cpe:2.3:a:realnetworks:realplayer:-:****:enterprise:****:
cpe:2.3:a:realnetworks:realplayer:10.0:****:****:
cpe:2.3:a:realnetworks:realplayer:10.0:****:linux:****:
cpe:2.3:a:realnetworks:realplayer:10.0:****:de:****:
cpe:2.3:a:realnetworks:realplayer:10.0:****:en:****:
cpe:2.3:a:realnetworks:realplayer:10.0:****:ja:****:
cpe:2.3:a:realnetworks:realplayer:10.0:beta:****:****:
cpe:2.3:a:realnetworks:realplayer:10.0:beta:****:mac_os_x:****:
cpe:2.3:a:realnetworks:realplayer:10.0_6.0.12.690:****:****:
cpe:2.3:a:realnetworks:realplayer:10.5:****:****:
cpe:2.3:a:realnetworks:realplayer:10.5_6.0.12.1016:beta:****:****:
cpe:2.3:a:realnetworks:realplayer:10.5_6.0.12.1040:****:****:
cpe:2.3:a:realnetworks:realplayer:8.0:****:****:
cpe:2.3:a:realnetworks:realplayer:8.0:****:mac_os_x:****:

cpe:2.3:a:realnetworks:realplayer:8.0:*:*:*:*:unix:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)