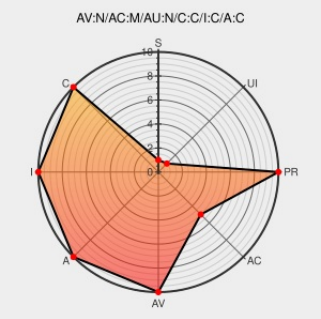
CVE-2010-4378

Published on: 12/14/2010 12:00:00 AM UTC

Last Modified on: 03/25/2021 11:02:29 PM UTC

CVE-2010-4378

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

The drv2.dll (aka RV20 decompression) module in RealNetworks RealPlayer 11.0 through 11.1, RealPlayer SP 1.0 through 1.1.5, RealPlayer Enterprise 2.1.2 and 2.1.3, Linux RealPlayer 11.0.2.1744, and possibly HelixPlayer 1.0.6 and other versions, allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via a crafted value of an unspecified length field in an RV20 video stream.

CVE-2010-4378 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
RealPlayer and StarSearch by Real Official Homepage — Real.com	Vendor Advisory, service.real.com, text/html	CONFIRM service.real.com/realplayer/security/12102010_player/en/
SecurityTracker.com Archives - RealPlayer Buffer Overflows and Memory Corruption Errors Let Remote Users Execute Arbitrary Code	www.securitytracker.com, text/html	SECTRACK 1024861
Support	www.redhat.com, text/html	REDHAT RHSA-2010:0981
Zero Day Initiative	www.zerodayinitiative.com, text/html	MISC www.zerodayinitiative.com/advisories/ZDI-10-274

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
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	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	11.0.3	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	2.1.2	All	enterprise	All
Application	Realnetworks	Realplayer	2.1.3	All	enterprise	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	11.0.3	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	2.1.2	All	enterprise	All
Application	Realnetworks	Realplayer	2.1.3	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
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

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:11.0:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:11.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:11.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:11.0.2.1744:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:11.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:11.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:11.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:11.1:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:2.1.2:*:enterprise:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:2.1.3:*:enterprise:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:11.0:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:11.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:11.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:11.0.2.1744:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:11.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:11.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:11.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:11.1:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:2.1.2:*:enterprise:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer:2.1.3:*:enterprise:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realplayer_sp:1.1.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→