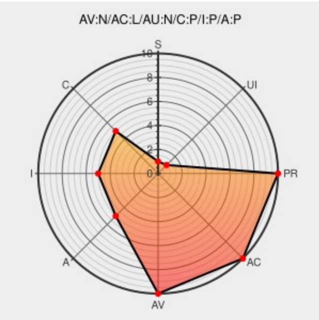
CVE-2002-1014

Published on: 10/04/2002 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:01 PM UTC

CVE-2002-1014

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



Certain versions of Realjukebox 2 from Realnetworks contain the following vulnerability:

Buffer overflow in RealJukebox 2 1.0.2.340 and 1.0.2.379, and RealOne Player Gold 6.0.10.505, allows remote attackers to execute arbitrary code via an RFS skin file whose skin.ini contains a long value in a CONTROLnImage argument, such as CONTROL1Image.

CVE-2002-1014 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
RealNetworks Support: Buffer Overrun Exploit	service.real.com text/html	CONFIRM service.real.com/help/faq/security/bufferoverrun07092002.html
CERT/CC Vulnerability Note VU#843667	US Government Resource www.kb.cert.org text/html	CERT-VN VU#843667
Real Networks RealJukebox/RealOne Player Gold Skinfile Buffer Overflow	Patch Vendor Advisory cve.report (archive) text/html	BID 5217
Neohapsis Archives - Bugtraq - [SPSadvisory#48]RealONE Player Gold / RealJukebox2 Buffer Overflow - From webmaster_at_shadowpenguin.org	archives.neohapsis.com text/x-c Inactive Link Not Archived	BUGTRAQ 20020712 [SPSadvisory#48]RealONE Player Gold / RealJukebox2 Buffer Overflow

ISS X-Force Database: realplayer-rjs-controlnimage-bo (9538): RealOne Player Gold and RealJukebox2 RJS skin file "CONTROLnImage" buffer overflow	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	XF realplayer-rjs-controlnimage-bo(9538)

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	Realjukebox 2	1.0.2.340	All	All	All
Application	Realnetworks	Realjukebox 2	1.0.2.379	All	All	All
Application	Realnetworks	Realjukebox 2	1.0.2.340	All	All	All
Application	Realnetworks	Realjukebox 2	1.0.2.379	All	All	All
Application	Realnetworks	Realjukebox 2 Plus	1.0.2.340	All	All	All
Application	Realnetworks	Realjukebox 2 Plus	1.0.2.379	All	All	All
Application	Realnetworks	Realjukebox 2 Plus	1.0.2.340	All	All	All
Application	Realnetworks	Realjukebox 2 Plus	1.0.2.379	All	All	All
Application	Realnetworks	Realone Player	6.0.10.505	gold	All	All
Application	Realnetworks	Realone Player	6.0.10.505	gold	All	All

cpe:2.3:a:realnetworks:realjukebox_2:1.0.2.340:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realjukebox_2:1.0.2.379:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realjukebox_2:1.0.2.340:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realjukebox_2:1.0.2.379:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realjukebox_2_plus:1.0.2.340:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realjukebox_2_plus:1.0.2.379:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realjukebox_2_plus:1.0.2.340:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realjukebox_2_plus:1.0.2.379:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realone_player:6.0.10.505:gold:*:*:*:*:*:

cpe:2.3:a:realnetworks:realone_player:6.0.10.505:gold:*:*:*:*:*:

No vendor comments have been submitted for this CVE