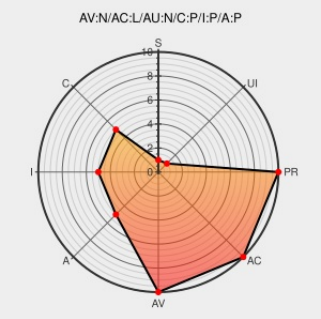
CVE-2003-1117

Published on: 12/31/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

CVE-2003-1117

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



Certain versions of Realsystem Proxy from Realnetworks contain the following vulnerability:

Buffer overflow in RealSystem Server 6.x, 7.x and 8.x, and RealSystem Proxy 8.x, related to URL error handling, allows remote attackers to cause a denial of service and possibly execute arbitrary code.

CVE-2003-1117 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
VU#912219 - RealSystem Proxy contains buffer overflow	US Government Resource, www.kb.cert.org, text/html	CERT-VN VU#912219
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF realsystem-malformed-url-bo(11362)
RealNetworks Support: Security Issues	Patch, service.real.com, text/html	CONFIRM service.real.com/help/faq/security/bufferoverflow.html
RealSystem Server and RealSystem Proxy Buffer Overflows May Let Remote Users Execute Arbitrary Code on the Server or Cause the Server to Crash - SecurityTracker	Patch, securitytracker.com, text/html	SECTRACK 1003604
CERT/CC Vulnerability Note VU#143627	Patch	CERT-VN VU#143627

Third Party Advisory
US Government Resource
www.kb.cert.org
text/html

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	Realsystem Proxy	8	All	All	All
Application	Realnetworks	Realsystem Proxy	8	All	All	All
Application	Realnetworks	Realsystem Server	6	All	All	All
Application	Realnetworks	Realsystem Server	7	All	All	All
Application	Realnetworks	Realsystem Server	8	All	All	All
Application	Realnetworks	Realsystem Server	6	All	All	All
Application	Realnetworks	Realsystem Server	7	All	All	All
Application	Realnetworks	Realsystem Server	8	All	All	All

cpe:2.3:a:realnetworks:realsystem_proxy:8:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realsystem_proxy:8:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realsystem_server:6:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realsystem_server:7:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realsystem_server:8:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realsystem_server:6:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realsystem_server:7:*:*:*:*:*:*:*:

cpe:2.3:a:realnetworks:realsystem_server:8:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report