CVE-2007-5601

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2007-5601
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-10-20 20:17:00 UTC
Updated	2017-07-29 01:33:00 UTC
Description	Stack-based buffer overflow in the Database Component in MPAMedia.dll in RealNetworks RealPlayer 10.5 and 11 beta, a

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Realnetworks	Realplayer	10.0	All	All	All
Application	Realnetworks	Realplayer	10.5	All	All	All
Application	Realnetworks	Realplayer	11_beta	All	All	All
Application	Realnetworks	Realplayer	10.0	All	All	All
Application	Realnetworks	Realplayer	10.5	All	All	All
Application	Realnetworks	Realplayer	11_beta	All	All	All

References

Reference	Source	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupe
RealPlayer ierpplug.dll ActiveX Control Import Playlist Name Stack Buffer Overflow Vulnerability	BID	www.secu
Symantec Security Response Weblog: RealPlayer Exploit On The Loose	MISC	www.syma
US-CERT Technical Cyber Security Alert TA07-297A -- RealNetworks RealPlayer ActiveX Playlist Buffer Overflow	CERT	www.us-c
NASA Bans IE? - Roger's Information Security Blog	MISC	www.infos
IBM X-Force Exchange	XF	exchange.
RealPlayer Input Validation Flaw in 'ierpplug.dll' Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	www.secu
RealPlayer and StarSearch by Real Official Homepage — Real.com	CONFIRM	service.re

RealPlayer Playlist Handling Buffer Overflow Vulnerability - Advisories - Secunia	SECUNIA	secunia.c
VU#871673 - RealPlayer playlist name stack buffer overflow	CERT-VN	www.kb.c
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-10-23	Mark J Cox	Not vulnerable. This issue did not affect versions of RealPlayer as shipped with Red Hat Enterpr

There are currently no legacy QID mappings associated with this CVE.