



CVE-2009-3670

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2009-3670
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-10-11 22:30:00 UTC
Updated	2017-09-19 01:29:00 UTC
Description	Stack-based buffer overflow in KSP Sound Player 2009 R2 and R2.1 allows remote attackers to execute arbitrary code via

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ksplayer	Ksp Sound Player	2009	r2	All	All
Application	Ksplayer	Ksp Sound Player	2009	r2.1	All	All
Application	Ksplayer	Ksp Sound Player	2009	r2	All	All
Application	Ksplayer	Ksp Sound Player	2009	r2.1	All	All

References

Reference	Source	Link
KSP 2009R2 (m3u) Universal Local Buffer Overflow Exploit (SEH)	EXPLOIT-DB	www.exploit-db.com/exploits/57983/
KSP Sound Player "m3u" Playlist Buffer Overflow - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com/advisories/57983/
57983	OSVDB	osvdb.org/57983
CVE Program record	CVE.ORG	www.cve.org/CVE-2009-3670
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2009-3670

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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