



# CVE-2012-6303

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

## Summary

<b>CVE</b>	CVE-2012-6303
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2013-10-28 22:55:00 UTC
<b>Updated</b>	2018-10-30 16:27:00 UTC
<b>Description</b>	Heap-based buffer overflow in the GetWavHeader function in generic/jkSoundFile.c in the Snack Sound Toolkit, as used in

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Kth</a>	<a href="#">Snack Sound Toolkit</a>	2.2.10	All	All	All
Application	<a href="#">Kth</a>	<a href="#">Snack Sound Toolkit</a>	2.2.10	All	All	All
Application	<a href="#">Kth</a>	<a href="#">Wavesurfer</a>	1.8.8	p4	All	All
Application	<a href="#">Kth</a>	<a href="#">Wavesurfer</a>	1.8.8	p4	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All

## References

Reference	Source	Link	Tags
Support / Security / Advisories // MDVSA-2013:126   Mandriva	MANDRIVA	<a href="http://www.mandriva.com">www.mandriva.com</a>	Broken Link
WaveSurfer 1.8.8p4 <= Memory Corruption PoC	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>	Exploit, VDB E
oss-security - CVE-2012-6303 WaveSurfer and Snack Sound Toolkit buffer overflows	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing List, Th
Gentoo Linux Documentation -- Snack: User-assisted execution of arbitrary code	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	Third Party Adv
[security-announce] openSUSE-SU-2015:0382-1: important: Security update	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	Third Party Adv
About Secunia Research   Flexera	SECUNIA	<a href="http://secunia.com">secunia.com</a>	Vendor Advisor

CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, anal

No vendor comments have been submitted for this CVE.

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

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)