



CVE-2018-17096

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

Summary

CVE	CVE-2018-17096
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-16 21:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	The BPMDetect class in BPMDetect.cpp in libSoundTouch.a in Olli Parviainen SoundTouch 2.0 allows remote attackers to

Risk And Classification

Problem Types: CWE-617

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Surina	Soundtouch	2.0.0	All	All	All
Application	Surina	Soundtouch	2.0.0	All	All	All

References

Reference	Source	Link	T
multiple asserstion failed and some other problems (#14) · Issues · SoundTouch library / soundtouch · GitLab	MISC	gitlab.com	T
pocs/soundtouch/2018_09_03 at master · TeamSeri0us/pocs · GitHub	MISC	github.com	E
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[501253](#) Alpine Linux Security Update for soundtouch

[670206](#) EulerOS Security Update for soundtouch (EulerOS-SA-2021-1705)

[670226](#) EulerOS Security Update for soundtouch (EulerOS-SA-2021-1849)

© [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](#)