



CVE-2007-6277

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

Summary

CVE	CVE-2007-6277
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-12-07 11:46:00 UTC
Updated	2018-10-15 21:51:00 UTC
Description	Multiple buffer overflows in Free Lossless Audio Codec (FLAC) libFLAC before 1.2.1 allow user-assisted remote attackers to

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Flac	Libflac	All	All	All	All

References

Reference	Source
SecurityTracker.com Archives - FLAC Buffer Overflows, Double Free Errors, and Other Bugs Let Remote Users Execute Arbitrary Code	SE
SecurityFocus	BU
SecurityReason - Multiple Vulnerabilities In .FLAC File Format and Various Media Applications	SR
Resources BeyondTrust	EE
US-CERT Vulnerability Note VU#544656	CE
Debian -- Security Information -- DSA-1469-1 flac	DE
Repository / Oval Repository	OV
Debian update for flac - Advisories - Secunia	SE
CVE Program record	CV
NVD vulnerability detail	NV

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](#)