



CVE-2004-0557

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

Summary

CVE	CVE-2004-0557
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-08-06 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Multiple buffer overflows in the st_wavstartread function in wav.c for Sound eXchange (SoX) 12.17.2 through 12.17.4 allow

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:C/A:C

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Conectiva	Linux	10.0	All	All	All

Operating System	Conectiva	Linux	8.0	All	All	All
Operating System	Conectiva	Linux	9.0	All	All	All
Operating System	Gentoo	Linux	1.4	All	All	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_servers	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Fedora Core	core_1.0	All	All	All
Operating System	Redhat	Fedora Core	core_2.0	All	All	All
Application	Sox	Sox	12.17.2	All	All	All
Application	Sox	Sox	12.17.3	All	All	All
Application	Sox	Sox	12.17.4	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference			Source		Link	
LWN: Fedora alert FEDORA-2004-244 (sox)			af854a3a-2127-422b-91ae-364da2661108		lwn.net	
redhat.com Red Hat Support			af854a3a-2127-422b-91ae-364da2661108		www.redhat	
Repository / Oval Repository			af854a3a-2127-422b-91ae-364da2661108		oval.cisecur	
Home - Conectiva			af854a3a-2127-422b-91ae-364da2661108		distro.conec	
Advisories - Mandriva			af854a3a-2127-422b-91ae-364da2661108		www.mandr	
bugzilla.fedora.us/show_bug.cgi			af854a3a-2127-422b-91ae-364da2661108		bugzilla.fede	
Debian -- Security Information -- DSA-565-1 sox			af854a3a-2127-422b-91ae-364da2661108		www.debiar	
IBM X-Force Exchange			af854a3a-2127-422b-91ae-364da2661108		exchange.x	
Full Disclosure: SoX buffer overflows when handling .WAV files			af854a3a-2127-422b-91ae-364da2661108		seclists.org	
Secunia - Advisories - SoX ".WAV" File Processing Buffer Overflow Vulnerabilities			af854a3a-2127-422b-91ae-364da2661108		secunia.com	
SoX WAV File Buffer Overflow Vulnerability			af854a3a-2127-422b-91ae-364da2661108		www.securi	
Gentoo Linux Documentation -- SoX: Multiple buffer overflows			af854a3a-2127-422b-91ae-364da2661108		www.gentoo	
archives.neohapsis.com/archives/vulnwatch/2004-q3/0014.html			af854a3a-2127-422b-91ae-364da2661108		archives.ne	
LWN: Fedora alert FEDORA-2004-235 (sox)			af854a3a-2127-422b-91ae-364da2661108		lwn.net	
CVE Program record			CVE.ORG		www.cve.or	
NVD vulnerability detail			NVD		nvd.nist.gov	

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](#)