



CVE-2016-10350

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

Summary

CVE	CVE-2016-10350
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-01 01:59:00 UTC
Updated	2018-12-28 16:29:00 UTC
Description	The archive_read_format_cab_read_header function in archive_read_support_format_cab.c in libarchive 3.2.2 allows remo

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libarchive	Libarchive	3.2.2	All	All	All
Application	Libarchive	Libarchive	3.2.2	All	All	All

References

Reference	Source	Link
libarchive: Multiple vulnerabilities (GLSA 201710-19) — Gentoo security	GENTOO	security.gentoo.org
heap-buffer-overflow in archive_read_format_cab_read_header · Issue #835 · libarchive/libarchive · GitHub	MISC	github.com
Debian -- Security Information -- DSA-4360-1 libarchive	DEBIAN	www.debian.org
USN-3736-1: libarchive vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
[SECURITY] [DLA 1600-1] libarchive security update	MLIST	lists.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710549](#) Gentoo Linux libarchive Multiple Vulnerabilities (GLSA 201710-19)

© [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](#)