



CVE-2016-1541

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

Summary

CVE	CVE-2016-1541
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-07 10:59:00 UTC
Updated	2018-01-05 02:30:00 UTC
Description	Heap-based buffer overflow in the zip_read_mac_metadata function in archive_read_support_format_zip.c in libarchive bef

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE	www.slack
openSUSE-SU-2016:1663-1: moderate: Security update for libarchive	SUSE	lists.oper
Issue #656: Fix CVE-2016-1541, VU#862384 · libarchive/libarchive@d0331e8 · GitHub	CONFIRM	github.co
Oracle Linux Bulletin - July 2016	CONFIRM	www.ora
Red Hat Customer Portal	REDHAT	rhn.redha
Debian -- Security Information -- DSA-3574-1 libarchive	DEBIAN	www.deb
Vulnerability Note VU#862384 - libarchive contains a heap-based buffer overflow due to improper input validation	CERT-VN	www.kb.c
openSUSE-SU-2016:1463-1: moderate: Security update for libarchive	SUSE	lists.oper
libarchive 'archive_read_support_format_zip.c' Heap Buffer Overflow Vulnerability	BID	www.sec
Vulnerable code, CVE-2016-1541 · Issue #656 · libarchive/libarchive · GitHub	CONFIRM	github.co
libarchive: Multiple vulnerabilities (GLSA 201701-03) — Gentoo security	GENTOO	security.g
USN-2981-1: libarchive vulnerabilities Ubuntu	UBUNTU	www.ubu
Oracle Solaris Bulletin - July 2016	CONFIRM	www.ora

CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
<p>No vendor comments have been submitted for this CVE.</p>		
<h3>Legacy QID Mappings</h3>		
<p>710502 Gentoo Linux libarchive Multiple Vulnerabilities (GLSA 201701-03)</p>		

© 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](#).

CVE.report and Source URL Uptime Status status.cve.report