



CVE-2019-14250

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

Summary

CVE	CVE-2019-14250
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-24 04:15:00 UTC
Updated	2023-03-01 18:01:00 UTC
Description	An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.32. simple_object_elf_match in simple-object-elf.

Risk And Classification

Problem Types: CWE-787 | CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Application	Gnu	Binutils	2.32	All	All	All
Application	Gnu	Binutils	2.32	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All

References

Reference	Source	Link	Tags
August 2019 GNU Binutils Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
[security-announce] openSUSE-SU-2019:2365-1: moderate: Security update f	SUSE	lists.opensuse.org	
USN-4326-1: libiberty vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	
[security-announce] openSUSE-SU-2020:1804-1: moderate: Security update f	SUSE	lists.opensuse.org	
[security-announce] openSUSE-SU-2020:0716-1: moderate: Security update f	SUSE	lists.opensuse.org	
USN-4336-1: GNU binutils vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	
GNU Binutils 'libiberty' CVE-2019-14250 Integer Overflow Vulnerability	BID	www.securityfocus.com	Third Party

Binutils: Multiple vulnerabilities (GLSA 202007-39) — Gentoo security	GENTOO	security.gentoo.org	
90924 – lto-plugin/lto-plugin.c heap memory corruption due to insufficient sanitization.	MISC	gcc.gnu.org	Exploit, Issue
Ren Kimura - [PATCH] libiberty: Check zero value shstrndx in simple-object-elf.c	MISC	gcc.gnu.org	Exploit, Mail
[security-announce] openSUSE-SU-2020:1790-1: moderate: Security update for binutils	SUSE	lists.opensuse.org	
[security-announce] openSUSE-SU-2019:2364-1: moderate: Security update for binutils	SUSE	lists.opensuse.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, e

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [377579](#) Alibaba Cloud Linux Security Update for binutils (ALINUX3-SA-2022:0120)
- [751313](#) SUSE Enterprise Linux Security Update for binutils (SUSE-SU-2021:3593-1)
- [752219](#) SUSE Enterprise Linux Security Update for gcc48 (SUSE-SU-2022:2015-1)
- [755898](#) SUSE Enterprise Linux Security Update for gcc7 (SUSE-SU-2023:3662-1)
- [900199](#) CBL-Mariner Linux Security Update for binutils 2.32
- [903694](#) Common Base Linux Mariner (CBL-Mariner) Security Update for binutils (1901)

© [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