



CVE-2020-35448

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-35448
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-27 04:15:00 UTC
Updated	2023-11-07 03:21:00 UTC
Description	An issue was discovered in the Binary File Descriptor (bfd) library (aka libbfd), as distributed in GNU Binutils 2.35.1. A heap

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Binutils	2.35.1	All	All	All
Application	Gnu	Binutils	2.35.1	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All

References

Reference	Source	Link	Tags
sourceware.org Git - binutils-gdb.git/commit		sourceware.org	
Binutils: Multiple vulnerabilities (GLSA 202107-24) — Gentoo security	GENTOO	security.gentoo.org	
26574 – A heap buffer overflow in bfd_getl_signed_32	MISC	sourceware.org	Exploit, Issue
sourceware.org Git - binutils-gdb.git/commit	MISC	sourceware.org	Patch, Third Party
CVE-2020-35448 GNU Binutils Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	Third Party
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159495 Oracle Enterprise Linux Security Update for binutils (ELSA-2021-4364)
239817 Red Hat Update for binutils (RHSA-2021:4364)
352841 Amazon Linux Security Advisory for gcc10-binutils: ALAS2-2021-1702
501880 Alpine Linux Security Update for mingw-w64-binutils
502041 Alpine Linux Security Update for binutils-cross-embedded
504587 Alpine Linux Security Update for binutils-cross-embedded
710052 Gentoo Linux Binutils Multiple vulnerabilities (GLSA 202107-24)
751313 SUSE Enterprise Linux Security Update for binutils (SUSE-SU-2021:3593-1)
751321 SUSE Enterprise Linux Security Update for binutils (SUSE-SU-2021:3616-1)
751331 OpenSUSE Security Update for binutils (openSUSE-SU-2021:3616-1)
751350 OpenSUSE Security Update for binutils (openSUSE-SU-2021:1475-1)
751916 SUSE Enterprise Linux Security Update for binutils (SUSE-SU-2022:0934-1)
940080 AlmaLinux Security Update for binutils (ALSA-2021:4364)
960767 Rocky Linux Security Update for binutils (RLSA-2021:4364)

© [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](#)