CVE-2021-20197

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-20197
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-26 17:15:00 UTC
Updated	2023-02-12 22:15:00 UTC
Description	There is an open race window when writing output in the following utilities in GNU binutils version 2.35 and earlier:ar, objco

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Broadcom	Brocade Fabric Operating System Firmware	-	All	All	All
Application	Gnu	Binutils	All	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Netapp	Solidfire Hci Management Node	-	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link
GNU Binutils: Multiple Vulnerabilities (GLSA 202208-30) — Gentoo security	GENTOO	security.gentoo.org
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com
26945 – Unsafe chown+chmod in smart_rename, possibly elsewhere	MISC	sourceware.org
1913743 – (CVE-2021-20197) CVE-2021-20197 binutils: race window allows users to own arbitrary files	MISC	bugzilla.redhat.com
CVE-2021-20197 GNU Binutils Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com
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

159495 Oracle Enterprise Linux Security Update for binutils (ELSA-2021-4364)

184238 Debian Security Update for binutils (CVE-2021-20197)

239817 Red Hat Update for binutils (RHSA-2021:4364)

670423 EulerOS Security Update for binutils (EulerOS-SA-2021-1976)

670442 EulerOS Security Update for binutils (EulerOS-SA-2021-2058)

670453 EulerOS Security Update for binutils (EulerOS-SA-2021-2047)

710599 Gentoo Linux GNU Binutils Multiple Vulnerabilities (GLSA 202208-30)

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)

900099 CBL-Mariner Linux Security Update for binutils 2.32

903491 Common Base Linux Mariner (CBL-Mariner) Security Update for binutils (4033)

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 registred 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