



CVE-2021-3800

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

Summary

CVE	CVE-2021-3800
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-23 16:15:00 UTC
Updated	2023-04-25 15:42:00 UTC
Description	A flaw was found in glib before version 2.63.6. Due to random charset alias, pkexec can leak content from files owned by p

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Gnome	Glib	All	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All

References

Reference	Source	Link
oss-security - charset.alias in pkexec/glib/gnulib (was: glibc locale issues)	MISC	www.openwall.com
[SECURITY] [DLA 3110-1] glib2.0 security update	MLIST	lists.debian.org
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com
CVE-2021-3800 GNOME GLib Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
libcharset: Drop a redundant environment variable (3529bb44) · Commits · GNOME / GLib · GitLab	MISC	gitlab.gnome.org
1938284 – (CVE-2021-3800) CVE-2021-3800 glib2: Possible privilege escalation through pkexec and aliases	MISC	bugzilla.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

[159502](#) Oracle Enterprise Linux Security Update for glib2 (ELSA-2021-4385)

[180967](#) Debian Security Update for glib2.0 (CVE-2021-3800)

[181058](#) Debian Security Update for glib2.0 (DLA 3110-1)

[198602](#) Ubuntu Security Notification for GLib Vulnerability (USN-5189-1)

[239790](#) Red Hat Update for glib2 (RHSA-2021:4385)

[354922](#) Amazon Linux Security Advisory for glib2 : ALAS-2023-1742

[355330](#) Amazon Linux Security Advisory for glib2 : ALAS2-2023-2058

[672605](#) EulerOS Security Update for glib2 (EulerOS-SA-2023-1315)

[672726](#) EulerOS Security Update for glib2 (EulerOS-SA-2023-1503)

[751864](#) SUSE Enterprise Linux Security Update for glib2 (SUSE-SU-2022:0828-1)

[903745](#) Common Base Linux Mariner (CBL-Mariner) Security Update for glib (10698)

[904760](#) Common Base Linux Mariner (CBL-Mariner) Security Update for glib (10698-1)

[940270](#) AlmaLinux Security Update for glib2 (ALSA-2021:4385)

[960672](#) Rocky Linux Security Update for glib2 (RLSA-2021:4385)

© [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](#)