



CVE-2021-4209

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

Summary

CVE	CVE-2021-4209
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-24 16:15:00 UTC
Updated	2022-10-27 16:57:00 UTC
Description	A NULL pointer dereference flaw was found in GnuTLS. As Nettle's hash update functions internally call memcpy, providing

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Gnutls	All	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Hci Bootstrap Os	-	All	All	All
Hardware	Netapp	Hci Compute Node	-	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
Null pointer dereference in MD_UPDATE (#1306) · Issues · gnutls / GnuTLS · GitLab	MISC	gitlab.
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	acces
wrap_nettle_hash_fast: avoid calling _update with zero-length input (!1503) · Merge requests · gnutls / GnuTLS · GitLab	MISC	gitlab.
CVE-2021-4209 GnuTLS Vulnerability in NetApp Products NetApp Product Security	CONFIRM	securi
wrap_nettle_hash_fast: avoid calling _update with zero-length input (3db35273) · Commits · gnutls / GnuTLS · GitLab	MISC	gitlab.
2044156 – (CVE-2021-4209) CVE-2021-4209 GnuTLS: Null pointer dereference in MD_UPDATE	MISC	bugzil
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

180842 Debian Security Update for gnutls28 (CVE-2021-4209)
180936 Debian Security Update for gnutls28 (DLA 3070-1)
198887 Ubuntu Security Notification for GnuTLS Vulnerabilities (USN-5550-1)
591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
672285 EulerOS Security Update for gnutls (EulerOS-SA-2022-2650)
672289 EulerOS Security Update for gnutls (EulerOS-SA-2022-2682)
672333 EulerOS Security Update for gnutls (EulerOS-SA-2022-2730)
672364 EulerOS Security Update for gnutls (EulerOS-SA-2022-2765)
672584 EulerOS Security Update for gnutls (EulerOS-SA-2023-1316)
672721 EulerOS Security Update for gnutls (EulerOS-SA-2023-1504)
751774 SUSE Enterprise Linux Security Update for gnutls (SUSE-SU-2022:0678-1)
751775 SUSE Enterprise Linux Security Update for gnutls (SUSE-SU-2022:0677-1)
751813 OpenSUSE Security Update for gnutls (openSUSE-SU-2022:0717-1)
752000 SUSE Enterprise Linux Security Update for gnutls (SUSE-SU-2022:0717-1)
752481 SUSE Enterprise Linux Security Update for gnutls (SUSE-SU-2022:2830-1)
903766 Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (10700)
904180 Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (10700-1)

© [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](#)