



CVE-2022-2509

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

Summary

CVE	CVE-2022-2509
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-01 14:15:00 UTC
Updated	2023-11-07 03:46:00 UTC
Description	A vulnerability found in gnutls. This security flaw happens because of a double free error occurs during verification of pkcs7

Risk And Classification

Problem Types: CWE-415

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Gnu	Gnutls	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-5203-1 gnutls28	DEBIAN	www.debian.org	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
[gnutls-help] gnutls 3.7.7	MISC	lists.gnupg.org	
[SECURITY] Fedora 35 Update: gnutls-3.7.7-1.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] [DLA 3070-1] gnutls28 security update	MLIST	lists.debian.org	
[SECURITY] Fedora 35 Update: gnutls-3.7.7-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160137 Oracle Enterprise Linux Security Update for gnutls and nettle (ELSA-2022-6854)
160169 Oracle Enterprise Linux Security Update for gnutls (ELSA-2022-7105)
180922 Debian Security Update for gnutls28 (DSA 5203-1)
180936 Debian Security Update for gnutls28 (DLA 3070-1)
182128 Debian Security Update for gnutls28 (CVE-2022-2509)
198887 Ubuntu Security Notification for GnuTLS Vulnerabilities (USN-5550-1)
240722 Red Hat Update for gnutls and nettle security (RHSA-2022:6854)
240778 Red Hat Update for gnutls (RHSA-2022:7105)
282995 Fedora Security Update for gnutls (FEDORA-2022-0156c442d0)
283043 Fedora Security Update for gnutls (FEDORA-2022-5470992bfc)
296084 Oracle Solaris 11.4 Support Repository Update (SRU) 50.126.3 Missing (CPUOCT2022)
377761 Alibaba Cloud Linux Security Update for gnutls (ALINUX3-SA-2022:0181)
502466 Alpine Linux Security Update for gnutls
502467 Alpine Linux Security Update for gnutls
503983 Alpine Linux Security Update for gnutls
591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
672179 EulerOS Security Update for gnutls (EulerOS-SA-2022-2461)
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)
690913 Free Berkeley Software Distribution (FreeBSD) Security Update for gnutls (1cd0c17a-17c0-11ed-91a5-080027f5fec9)
752481 SUSE Enterprise Linux Security Update for gnutls (SUSE-SU-2022:2830-1)
752504 SUSE Enterprise Linux Security Update for gnutls (SUSE-SU-2022:2882-1)
752515 SUSE Enterprise Linux Security Update for gnutls (SUSE-SU-2022:2919-1)

902648 Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (10438)
902658 Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (10439)
903792 Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (10439-1)
904749 Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (10438-1)
940666 AlmaLinux Security Update for gnutls and nettle (ALSA-2022:6854)
940717 AlmaLinux Security Update for gnutls (ALSA-2022:7105)
960441 Rocky Linux Security Update for gnutls (RLSA-2022:7105)
960648 Rocky Linux Security Update for gnutls and nettle (RLSA-2022:6854)

© [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](#)