



CVE-2023-25824

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

Summary

CVE	CVE-2023-25824
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-23 22:15:00 UTC
Updated	2023-11-07 04:09:00 UTC
Description	Mod_gnutls is a TLS module for Apache HTTPD based on GnuTLS. Versions from 0.9.0 to 0.12.0 (including) did not proper

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mod Gnutls Project	Mod Gnutls	All	All	All	All
Application	Mod Gnutls Project	Mod Gnutls	All	All	All	All

References

Reference	Source	Link	Tags
#942737 - libapache2-mod-gnutls: mod_gnutls consumes 100% cpu - Debian Bug report logs	MISC	bugs.debian.org	
Fix loop in blocking read on transport timeout · airtower-luna/mod_gnutls@d7eec4e · GitHub	MISC	github.com	
Infinite Loop on request read timeout in mod_gnutls · Advisory · airtower-luna/mod_gnutls · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[691146](#) Free Berkeley Software Distribution (FreeBSD) Security Update for mod_gnutls (e8b20517-dbb6-11ed-bf28-589cfc0f81b0)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)