Gnutls: gnutls: denial of service via excessive resource consumption during certificate verification

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-14831
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-09 15:16:09 UTC
Updated	2026-04-22 19:16:59 UTC
Description	A flaw was found in GnuTLS. This vulnerability allows a denial of service (DoS) by excessive CPU (Central Processing Unit

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from secalert@redhat.com

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

EPSS: 0.000590000 probability, percentile 0.183880000 (date 2026-04-22)

Problem Types: CWE-407 | CWE-407 Inefficient Algorithmic Complexity

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:3.8.10-3.el10_1 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 10.0 Extended Update Support	unaffected 0:3.8.9-9.el10_0.17 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:3.6.16-8.el8_10.5 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:3.6.16-8.el8_10.5 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:3.8.3-10.el9_7 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:3.8.3-10.el9_7 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:3.7.6-21.el9_2.5 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:3.8.3-4.el9_4.5 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.6 Extended Update Support	unaffected 0:3.8.3-6.el9_6.3 * rpm
CNA	Red Hat	Red Hat AI Inference Server 3.2	unaffected sha256:54616c9f3e4d27120504b0b2020
CNA	Red Hat	Red Hat AI Inference Server 3.3	unaffected sha256:0ec114881d9dcd28a5dbbb2ec0e
CNA	Red Hat	Red Hat AI Inference Server 3.3	unaffected sha256:813ba7ccd1696b44deb90d9e6cc
CNA	Red Hat	Red Hat AI Inference Server 3.3	unaffected sha256:be6d568f28044533e4ad80f0856
CNA	Red Hat	Red Hat Ceph Storage 8	unaffected sha256:1160569002c25d3d349bbe41b57
CNA	Red Hat	Red Hat Discovery 2	unaffected sha256:040dadd657afdb9f0914f896a496
CNA	Red Hat	Red Hat Discovery 2	unaffected sha256:062310de4b34e278f8c7e4634de
CNA	Red Hat	Red Hat Hardened Images	unaffected 3.8.12-1.1.hum1 * rpm
CNA	Red Hat	Red Hat Insights Proxy 1.5	unaffected sha256:325c34e2506d715975171557d40
CNA	Red Hat	Red Hat Update Infrastructure 5	unaffected sha256:200c27e9b396276bd505c6b4112
CNA	Red Hat	Red Hat Update Infrastructure 5	unaffected sha256:d98fd3fe5f5f9acd0efae7db19b61
CNA	Red Hat	Red Hat Update Infrastructure 5	unaffected sha256:2c50c87906a1abebf427a70f401c
CNA	Red Hat	Red Hat Update Infrastructure 5	unaffected sha256:5f1fbf66fb349a7baf066a1216d39
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified

References

Reference	Source	Link	Tags

access.redhat.com/errata/RHSA-2026:6618	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:5606	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:8747	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:6738	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/errata/RHSA-2026:4188	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:7329	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:8748	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:6630	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:6737	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4943	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4655	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:3477	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:7335	secalert@redhat.com	access.redhat.com	
gitlab.com/gnutls/gnutls/-/issues/1773	secalert@redhat.com	gitlab.com	
access.redhat.com/security/cve/CVE-2025-14831	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:8746	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:7477	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:5585	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-12-17T14:48:30.222Z	Reported to Red Hat.
CNA	2026-02-09T14:26:34.939Z	Made public.

There are currently no legacy QID mappings associated with this CVE.

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**