Gnutls: null pointer dereference in _gnutls_figure_common_ciphersuite()

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

Summary

CVE	CVE-2025-6395
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-07-10 16:15:25 UTC
Updated	2026-04-23 18:16:22 UTC
Description	A NULL pointer dereference flaw was found in the GnuTLS software in _gnutls_figure_common_ciphersuite().

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from secalert@redhat.com

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

EPSS: 0.000730000 probability, percentile 0.220820000 (date 2026-04-23)

Problem Types: CWE-476 | CWE-476 NULL Pointer Dereference

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:H
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat Enterprise Linux 10	unaffected 0:3.8.9-9.el10_0.14 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:3.6.16-8.el8_10.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 8	unaffected 0:3.6.16-8.el8_10.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:3.8.3-6.el9_6.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9	unaffected 0:3.8.3-6.el9_6.2 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions	unaffected 0:3.7.6-21.el9_2.4 * rpm
CNA	Red Hat	Red Hat Enterprise Linux 9.4 Extended Update Support	unaffected 0:3.8.3-4.el9_4.4 * rpm
CNA	Red Hat	Red Hat Ceph Storage 7	unaffected sha256:4d2f9dc5b2b33ee1c77bbfabcbbb
CNA	Red Hat	Red Hat Discovery 2	unaffected sha256:435ba9959b793d46a63a74c343
CNA	Red Hat	Red Hat Insights Proxy 1.5	unaffected sha256:4ca38b33efec0d2dd17a8fd822a7
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
lists.debian.org/debian-lts-announce/2025/08/msg00005.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	
access.redhat.com/errata/RHSA-2025:22529	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:16115	secalert@redhat.com	access.redhat.com	
www.openwall.com/lists/oss-security/2025/07/11/3	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
access.redhat.com/errata/RHSA-2025:17415	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2025-6395	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:17361	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:16116	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:17181	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2025:17348	secalert@redhat.com	access.redhat.com	
gitlab.com/gnutls/gnutls/-/issues/1718	secalert@redhat.com	gitlab.com	

access.redhat.com/errata/RHSA-2025:19088	secalert@redhat.com	access.redhat.com	
lists.gnupg.org/pipermail/gnutls-help/2025-July/004883.html	secalert@redhat.com	lists.gnupg.org	
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.

Additional Advisory Data

Source	Time	Event
CNA	2025-07-07T09:30:13.037Z	Reported to Red Hat.
CNA	2025-07-10T07:56:53.029Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

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