Gnutls: vulnerability in gnutls sct extension parsing

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

Summary

CVE	CVE-2025-32989
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-07-10 08:15:24 UTC
Updated	2026-04-14 11:16:24 UTC
Description	A heap-buffer-overread vulnerability was found in GnuTLS in how it handles the Certificate Transparency (CT) Signed Certi

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:L/I:N/A:N

EPSS: 0.001410000 probability, percentile 0.343230000 (date 2026-04-15)

Problem Types: CWE-295 | CWE-295 Improper Certificate Validation

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:L/I:N/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Gnutls	-	All	All	All
Operating System	Redhat	Enterprise Linux	10.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All

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 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 sha256:435ba9959b793d46a63a74c343b
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 Enterprise Linux 8	Not specified
CNA	Red Hat	Red Hat Hardened Images	Not specified
CNA	Red Hat	Red Hat OpenShift Container Platform 4	Not specified

References

Reference	Source	Link	Tags
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/security/cve/CVE-2025-32989	secalert@redhat.com	access.redhat.com	Vendor Advi
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	
access.redhat.com/errata/RHSA-2025:19088	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Tracki
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, a

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-04-15T01:21:36.512Z	Reported to Red Hat.
CNA	2025-07-10T07:54:13.541Z	Made public.

Workarounds

CNA: Currently, no mitigation is available for this vulnerability.

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