Gnutls: stack-based buffer overflow in gnutls_pkcs11_token_init() function

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

Summary

CVE	CVE-2025-9820
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-26 20:16:09 UTC
Updated	2026-04-22 02:16:01 UTC
Description	A flaw was found in the GnuTLS library, specifically in the gnutls_pkcs11_token_init() function that handles PKCS#11 token

Risk And Classification

Primary CVSS: v3.1 4 MEDIUM from secalert@redhat.com

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

EPSS: 0.000090000 probability, percentile 0.009650000 (date 2026-04-22)

Problem Types: CWE-121 | CWE-121 Stack-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	CVSS	4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

Availability

Low

CVSS:3.1/AV:L/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 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 Ceph Storage 8	unaffected sha256:1160569002c25d3d349bbe41b57eeffade438853d3419ed
CNA	Red Hat	Red Hat Discovery 2	unaffected sha256:040dadd657afdb9f0914f896a4962fd3dbf40b70c8037e4d7
CNA	Red Hat	Red Hat Discovery 2	unaffected sha256:062310de4b34e278f8c7e4634def673a77d1228d493541ef
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 sha256:325c34e2506d715975171557d40afb449c79cf6e0c41b357
CNA	Red Hat	Red Hat Update Infrastructure 5	unaffected sha256:200c27e9b396276bd505c6b41127ac5eb1d94d620172cb8
CNA	Red Hat	Red Hat Update Infrastructure 5	unaffected sha256:d98fd3fe5f5f9acd0efae7db19b61b864be1eb2fbe2586a1b
CNA	Red Hat	Red Hat Update Infrastructure 5	unaffected sha256:2c50c87906a1abebf427a70f401c409f1258cb55d2096f517
CNA	Red Hat	Red Hat Update Infrastructure 5	unaffected sha256:5f1fbf66fb349a7baf066a1216d39989c3b89f18ec5108b96
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
access.redhat.com/errata/RHSA-2026:5606	secalert@redhat.com	access.redha
www.openwall.com/lists/oss-security/2025/11/20/2	af854a3a-2127-422b-91ae-364da2661108	www.openwa
gitlab.com/gnutls/gnutls/-/issues/1732	secalert@redhat.com	gitlab.com
www.gnutls.org/security-new.html	secalert@redhat.com	www.gnutls.o
access.redhat.com/errata/RHSA-2026:4188	secalert@redhat.com	access.redha
access.redhat.com/security/cve/CVE-2025-9820	secalert@redhat.com	access.redha
access.redhat.com/errata/RHSA-2026:7329	secalert@redhat.com	access.redha
access.redhat.com/errata/RHSA-2026:4943	secalert@redhat.com	access.redha

bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redha
access.redhat.com/errata/RHSA-2026:4655	secalert@redhat.com	access.redha
access.redhat.com/errata/RHSA-2026:3477	secalert@redhat.com	access.redha
access.redhat.com/errata/RHSA-2026:7477	secalert@redhat.com	access.redha
access.redhat.com/errata/RHSA-2026:5585	secalert@redhat.com	access.redha
gitlab.com/gnutls/gnutls/-/commit/1d56f96f6ab5034d677136b9d50b5a75dff0faf5	secalert@redhat.com	gitlab.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2025-09-02T10:00:18.839Z	Reported to Red Hat.
CNA	2025-11-18T00:00:00.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options don't meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability. Applying the upstream patch or vendor-supplied security update is the recommended resolution.

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