



# Bug 2392528 (CVE-2025-9820) - CVE-2025-9820 gnutls: Stack-based Buffer Overflow in gnutls\_pkcs11\_token\_init() Function

**Keywords:** Security

**Reported:** 2025-09-02 10:07 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2026-04-09 13:20 UTC ([History](#))

**Alias:** CVE-2025-9820

**CC List:** 6 users ([show](#))

**Product:** Security Response

**Fixed In Version:**

**Component:** vulnerability

**Clone Of:**

**Environment:**

**Version:** unspecified

**Last Closed:**

**Embargoed:**

**Hardware:** All

**OS:** Linux

**Priority:** low

**Severity:** low

**Target Milestone:** ---

**Assignee:** Product Security DevOps Team

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:**

**Blocks:**


**TreeView+** [depends on](#) / [blocked](#)

Attachments	<a href="#">(Terms of Use)</a>

## Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	<a href="#">RHBA-2026:4361</a>	0	None	None	None	2026-03-11 15:36:09 UTC
Red Hat Product Errata	<a href="#">RHBA-2026:4478</a>	0	None	None	None	2026-03-12 13:09:57 UTC
Red Hat Product Errata	<a href="#">RHBA-2026:4485</a>	0	None	None	None	2026-03-12 13:21:41 UTC

Red Hat Product Errata	<a href="#">RHBA-2026:4486</a>	0	None	None	None	2026-03-12 15:05:12 UTC
Red Hat Product Errata	<a href="#">RHBA-2026:5650</a>	0	None	None	None	2026-03-24 16:23:38 UTC
Red Hat Product Errata	<a href="#">RHBA-2026:5654</a>	0	None	None	None	2026-03-24 16:48:06 UTC
Red Hat Product Errata	<a href="#">RHBA-2026:5820</a>	0	None	None	None	2026-03-25 14:36:36 UTC
Red Hat Product Errata	<a href="#">RHBA-2026:5839</a>	0	None	None	None	2026-03-25 17:50:17 UTC
Red Hat Product Errata	<a href="#">RHBA-2026:6197</a>	0	None	None	None	2026-03-30 17:24:12 UTC
Red Hat Product Errata	<a href="#">RHBA-2026:6258</a>	0	None	None	None	2026-03-31 12:32:28 UTC
Red Hat Product Errata	<a href="#">RHBA-2026:6479</a>	0	None	None	None	2026-04-02 14:15:44 UTC
Red Hat Product Errata	<a href="#">RHBA-2026:7043</a>	0	None	None	None	2026-04-08 12:44:11 UTC
Red Hat Product Errata	<a href="#">RHBA-2026:7297</a>	0	None	None	None	2026-04-09 13:20:16 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:3477</a>	0	None	None	None	2026-03-02 01:32:52 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:4188</a>	0	None	None	None	2026-03-10 23:26:32 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:5585</a>	0	None	None	None	2026-03-24 10:24:58 UTC

OSIDB Bzimport  2025-09-02 10:07:03 UTC[Description](#)

Stack-based buffer overflow vulnerability in the PKCS#11 token initialization function `gnutls_pkcs11_token_init()` of the GnuTLS library. The flaw is caused by an unsafe `memcpy` into a fixed-size stack buffer (`flabel[32]`) without proper bounds checking. If an attacker provides a token label longer than 32 bytes, it leads to out-of-bounds memory writes, causing a crash or, in some environments, potential code execution. Although the vulnerability requires local access or interaction with a malicious PKCS#11 token, it poses a security risk by enabling denial-of-service or possible privilege escalation in applications relying on GnuTLS.

errata-xmlrpc 2026-03-02 01:32:50 UTC

[Comment 1](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 10

Via RHSA-2026:3477 <https://access.redhat.com/errata/RHSA-2026:3477>

errata-xmlrpc 2026-03-10 23:26:31 UTC

[Comment 2](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9

Via RHSA-2026:4188 <https://access.redhat.com/errata/RHSA-2026:4188>

errata-xmlrpc 2026-03-24 10:24:56 UTC

[Comment 3](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via RHSA-2026:5585 <https://access.redhat.com/errata/RHSA-2026:5585>

---

Note

You need to [log in](#) before you can comment on or make changes to this bug.

