Bug 2359621 (CVE-2025-32989) - CVE-2025-32989 gnutls: Vulnerability in GnuTLS SCT extension parsing

Keywords:

Status: NEW

Alias: CVE-2025-32989

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2025-04-15 01:32 UTC by OSIDB Bzimport

Modified: 2026-02-23 23:00 UTC (History)

CC List: 7 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHBA-2025:16243	0	None	None	None	2025-09-18 18:45:09 UTC
Red Hat Product Errata	RHBA-2025:16265	0	None	None	None	2025-09-22 01:16:16 UTC
Red Hat Product Errata	RHBA-2025:16484	0	None	None	None	2025-09-23 15:35:14 UTC

Red Hat Product Errata	RHBA-2025:17455	0	None	None	None	2025-10-07 12:57:56 UTC
Red Hat Product Errata	RHBA-2025:17491	0	None	None	None	2025-10-07 13:02:28 UTC
Red Hat Product Errata	RHBA-2025:17492	0	None	None	None	2025-10-07 13:00:31 UTC
Red Hat Product Errata	RHBA-2025:17497	0	None	None	None	2025-10-07 15:45:23 UTC
Red Hat Product Errata	RHSA-2025:16115	0	None	None	None	2025-09-17 17:06:43 UTC
Red Hat Product Errata	RHSA-2025:16116	0	None	None	None	2025-09-17 17:59:15 UTC
Red Hat Product Errata	RHSA-2025:17348	0	None	None	None	2025-10-06 02:29:24 UTC
Red Hat Product Errata	RHSA-2025:17361	0	None	None	None	2025-10-06 08:43:17 UTC

OSIDB Bzimport 2025-04-15 01:32:21 UTC Description

```
A heap-buffer-overread vulnerability exists in GnuTLS
(confirmed in version 3.8.9) due to unsafe
handling of the Certificate Transparency (CT) Signed
Certificate Timestamp (SCT) extension
during X.509 certificate parsing. The vulnerability can be
triggered by a malicious peer
presenting a crafted certificate containing a malformed SCT
extension (OID
1.3.6.1.4.1.11129.2.4.2).
This overread may lead to disclosure of heap memory contents
to attackers if the SCT log_id
is logged, exported, or otherwise exposed by the application
consuming the GnuTLS client
library.
```

errata-xmlrpc 2025-09-17 17:06:41 UTC Comment 2

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 10

Via RHSA-2025:16115 https://access.redhat.com/errata/RHSA-2025:16115

errata-xmlrpc 2025-09-17 17:59:14 UTC Comment 3

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2025:16116 https://access.redhat.com/errata/RHSA-2025:16116

errata-xmlrpc 2025-10-06 02:29:22 UTC Comment 4

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2025:17348 https://access.redhat.com/errata/RHSA-2025:17348

errata-xmlrpc 2025-10-06 08:43:15 UTC Comment 5

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.2 Update Services for SAP Solutions

Via RHSA-2025:17361 https://access.redhat.com/errata/RHSA-2025:17361

Note

You need to log in before you can comment on or make changes to this bug.