Bug 2423177 (CVE-2025-14831) - CVE-2025-14831 gnutls: GnuTLS: Denial of Service via excessive resource consumption during certificate verification

Keywords: Security

Status: NEW

Alias: CVE-2025-14831

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: ~~2437986~~ ~~2437987~~

Blocks:

TreeView+ depends on / blocked

Reported: 2025-12-17 14:52 UTC by OSIDB Bzimport

Modified: 2026-04-09 13:20 UTC (History)

CC List: 6 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-2026:4361	0	None	None	None	2026-03-11 15:36:08 UTC
Red Hat Product Errata	RHBA-2026:4478	0	None	None	None	2026-03-12 13:10:00 UTC
Red Hat Product Errata	RHBA-2026:4485	0	None	None	None	2026-03-12 13:21:44 UTC

Red Hat Product Errata	RHBA-2026:4486	0	None	None	None	2026-03-12 15:05:13 UTC
Red Hat Product Errata	RHBA-2026:5650	0	None	None	None	2026-03-24 16:23:36 UTC
Red Hat Product Errata	RHBA-2026:5654	0	None	None	None	2026-03-24 16:48:04 UTC
Red Hat Product Errata	RHBA-2026:5820	0	None	None	None	2026-03-25 14:36:35 UTC
Red Hat Product Errata	RHBA-2026:5839	0	None	None	None	2026-03-25 17:50:16 UTC
Red Hat Product Errata	RHBA-2026:6197	0	None	None	None	2026-03-30 17:24:10 UTC
Red Hat Product Errata	RHBA-2026:6258	0	None	None	None	2026-03-31 12:32:30 UTC
Red Hat Product Errata	RHBA-2026:6479	0	None	None	None	2026-04-02 14:15:44 UTC
Red Hat Product Errata	RHBA-2026:7043	0	None	None	None	2026-04-08 12:44:12 UTC
Red Hat Product Errata	RHBA-2026:7297	0	None	None	None	2026-04-09 13:20:15 UTC
Red Hat Product Errata	RHSA-2026:3477	0	None	None	None	2026-03-02 01:32:52 UTC
Red Hat Product Errata	RHSA-2026:4188	0	None	None	None	2026-03-10 23:26:33 UTC
Red Hat Product Errata	RHSA-2026:5585	0	None	None	None	2026-03-24 10:24:58 UTC
Red Hat	RHSA-2026:6618	0	None	None	None	2026-04-06

Product Errata						03:24:37 UTC
Red Hat Product Errata	RHSA-2026:6630	0	None	None	None	2026-04-06 07:01:23 UTC
Red Hat Product Errata	RHSA-2026:6737	0	None	None	None	2026-04-07 07:50:00 UTC
Red Hat Product Errata	RHSA-2026:6738	0	None	None	None	2026-04-07 07:53:33 UTC

OSIDB Bzimport 2025-12-17 14:52:47 UTC Description

```
Verifying Certificates with large amout of name constraints
and subject alternative names makes GnuTLS vulnerable to DoS
attacks

When trying to verify a certificate chain using the certtool -
-verify command, with certificates, that contain a larger
number of SANs and Name Constraints, GnuTLS tries to verify
all of them, without any bound on the quantity of those
fields.
Using those crafted malicious certificate, GnuTLS is
vulnerable to DoS attacks by excessive usage of CPU and
memory.
```

errata-xmlrpc 2026-03-02 01:32:50 UTC Comment 2

```
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 3

```
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 10:24:57 UTC Comment 4

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

errata-xmlrpc 2026-04-06 03:24:36 UTC Comment 5

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 10.0 Extended Update Support

Via RHSA-2026:6618 https://access.redhat.com/errata/RHSA-2026:6618

errata-xmlrpc 2026-04-06 07:01:21 UTC Comment 6

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.6 Extended Update Support

Via RHSA-2026:6630 https://access.redhat.com/errata/RHSA-2026:6630

errata-xmlrpc 2026-04-07 07:49:58 UTC Comment 7

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.2 Update Services for SAP Solutions

Via RHSA-2026:6737 https://access.redhat.com/errata/RHSA-2026:6737

errata-xmlrpc 2026-04-07 07:53:32 UTC Comment 8

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2026:6738 https://access.redhat.com/errata/RHSA-

2026:6738

Note

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