



# Gnutls: gnutls: authentication bypass via nul character in username

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2026-42010  |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | redhat  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2026-05-07 12:16:17 UTC   |
| <b>Updated</b>         | 2026-05-07 15:16:09 UTC   |
| <b>Description</b>     | A flaw was found in gnutls. Servers configured with RSA-PSK (Rivest–Shamir–Adleman – Pre-Shared Key) wrongfully mat |

## Risk And Classification

**Primary CVSS:** v3.1 7.1 HIGH from secalert@redhat.com

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

**Problem Types:** CWE-626 | CWE-626 CWE-626 Null Byte Interaction Error (Poison Null Byte)

| Version | Source              | Type      | Score | Severity | Vector                                       |
|---------|---------------------|-----------|-------|----------|--|
| 3.1     | secalert@redhat.com | Secondary | 7.1   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N |
| 3.1     | CNA                 | CVSS      | 7.1   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N |

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**Low**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

**High**

Integrity

Low

Availability

None

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

### Vendor Declared Affected Products

| Source | Vendor  | Product                                | Version       | Platforms     |
|--------|---------|--|---------------|---------------|
| CNA    | Red Hat | Red Hat Enterprise Linux 10            | Not specified | Not specified |
| CNA    | Red Hat | Red Hat Enterprise Linux 6             | Not specified | Not specified |
| CNA    | Red Hat | Red Hat Enterprise Linux 7             | Not specified | Not specified |
| CNA    | Red Hat | Red Hat Enterprise Linux 8             | Not specified | Not specified |
| CNA    | Red Hat | Red Hat Enterprise Linux 9             | Not specified | Not specified |
| CNA    | Red Hat | Red Hat Hardened Images                | Not specified | Not specified |
| CNA    | Red Hat | Red Hat OpenShift Container Platform 4 | Not specified | Not specified |

### References

| Reference                                     | Source              | Link                | Tags                |
|---|---------------------|---------------------|---------------------|
| bugzilla.redhat.com/show_bug.cgi              | secalert@redhat.com | bugzilla.redhat.com |                     |
| access.redhat.com/security/cve/CVE-2026-42010 | secalert@redhat.com | access.redhat.com   |                     |
| CVE Program record                            | CVE.ORG             | www.cve.org         | canonical           |
| NVD vulnerability detail                      | NVD                 | nvd.nist.gov        | canonical, analysis |

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** Red Hat would like to thank Joshua Rogers (AISLE Research Team) for reporting this issue. (en)

### Additional Advisory Data

| Source | Time                     | Event                |
|--------|--------------------------|----------------------|
| CNA    | 2026-05-06T16:57:37.044Z | Reported to Red Hat. |
| CNA    | 2026-04-29T00:00:00.000Z | Made public.         |

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)