



# SUNRPC: Fix loop termination condition in gss\_free\_in\_token\_pages()

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

## Summary

<b>CVE</b>	CVE-2024-36288
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-06-21 12:15:10 UTC
<b>Updated</b>	2026-05-12 12:16:48 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: SUNRPC: Fix loop termination condition in gss\_free\_in\_to

## Risk And Classification

**Primary CVSS:** v3.1 5.5 MEDIUM from nvd@nist.gov

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

**EPSS:** 0.000080000 probability, percentile 0.007150000 (date 2026-05-12)

**Problem Types:** CWE-835

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	6.10.0	rc1	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected ab8466d4e26806a4ae82c282762c4545eecf
CNA	Linux	Linux	affected 4420b73c7f26fd5fcb37bbce5313dd356ef1b3
CNA	Linux	Linux	affected f148a95f68c66c1b097391b68e153d5a46f0e
CNA	Linux	Linux	affected fe0b474974fee7af1df286e0edd5a1460c811f
CNA	Linux	Linux	affected c1d8c429e4d2ce85ec5c92cf71cb419baf75c
CNA	Linux	Linux	affected 8ca148915670a2921afcc255af9e1dc80f37b
CNA	Linux	Linux	affected bafa6b4d95d97877baa61883ff90f7e374427f
CNA	Linux	Linux	affected a3c1afd5d7ad59e34a275d80c428952f83c8c
CNA	Linux	Linux	affected 6.9.3 6.9.4 semver
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.1 custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	unaffected * custom
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	affected V3.1 custom
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

### References

Reference	Source	Link
git.kernel.org/stable/c/6ed45d20d30005bed94c8c527ce51d5ad8121018	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/57ff6c0a175930856213b2aa39f8c845a53e5b1c	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/0a1cb0c6102bb4fd310243588d39461da49497ad	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/4a77c3dead97339478c7422eb07bf4bf63577008	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>
git.kernel.org/stable/c/f9977e4e0cd98a5f06f2492b4f3547db58deabf5	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
cert-portal.siemens.com/productcert/html/ssa-613116.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>
git.kernel.org/stable/c/b4878ea99f2b40ef1925720b1b4ca7f4af1ba785	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/af628d43a822b78ad8d4a58d8259f8bf8bc71115	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>
lists.debian.org/debian-lts-announce/2024/06/msg00020.html	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>
git.kernel.org/stable/c/4cefcd0af7458bdeff56a9d8dfc6868ce23d128a	af854a3a-2127-422b-91ae-364da2661108	<a href="https://git.kernel.org">git.kernel.org</a>

CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

© [CVE.report](http://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

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

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)