



scsi: iscsi_tcp: Fix UAF during logout when accessing the shost ipaddress

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

Summary

CVE	CVE-2023-52975
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-03-27 17:15:44 UTC
Updated	2026-04-01 18:09:42 UTC

Description In the Linux kernel, the following vulnerability has been resolved: scsi: iscsi_tcp: Fix UAF during logout when accessing the

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from ADP

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

Problem Types: CWE-416 | CWE-416 CWE-416 Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected a79af8a64d395bd89de8695a5ea5e1a7f01f02a8 0af745fddefbd56198f4f35eb309215ee5f9e21e git
CNA	Linux	Linux	affected a79af8a64d395bd89de8695a5ea5e1a7f01f02a8 17b738590b97fb3fc287289971d1519ff9b875a1 git
CNA	Linux	Linux	affected a79af8a64d395bd89de8695a5ea5e1a7f01f02a8 8859687f5b242c0b057461df0a9ff51d5500783b git
CNA	Linux	Linux	affected a79af8a64d395bd89de8695a5ea5e1a7f01f02a8 6f1d64b13097e85abda0f91b5638000afc5f9a06 git
CNA	Linux	Linux	affected 2.6.39
CNA	Linux	Linux	unaffected 2.6.39 semver
CNA	Linux	Linux	unaffected 5.10.248 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.93 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.11 6.1.* semver
CNA	Linux	Linux	unaffected 6.2 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/17b738590b97fb3fc287289971d1519ff9b875a1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/6f1d64b13097e85abda0f91b5638000afc5f9a06	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/8859687f5b242c0b057461df0a9ff51d5500783b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/0af745fddefbd56198f4f35eb309215ee5f9e21e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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