Kernel use-after-free bug in the TIOCNOTTY handler

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-5398
State	PUBLISHED
Assigner	freebsd
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 03:16:01 UTC
Updated	2026-05-01 12:49:44 UTC
Description	The implementation of TIOCNOTTY failed to clear a back-pointer from the structure representing the controlling terminal to

Risk And Classification

Primary CVSS: v3.1 8.4 HIGH from ADP

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

EPSS: 0.000170000 probability, percentile 0.042940000 (date 2026-05-05)

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

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/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	Freebsd	Freebsd	13.5	-	All	All
Operating System	Freebsd	Freebsd	13.5	beta3	All	All
Operating System	Freebsd	Freebsd	13.5	p1	All	All
Operating System	Freebsd	Freebsd	13.5	p10	All	All
Operating System	Freebsd	Freebsd	13.5	p11	All	All
Operating System	Freebsd	Freebsd	13.5	p2	All	All
Operating System	Freebsd	Freebsd	13.5	p3	All	All
Operating System	Freebsd	Freebsd	13.5	p4	All	All
Operating System	Freebsd	Freebsd	13.5	p5	All	All
Operating System	Freebsd	Freebsd	13.5	p6	All	All
Operating System	Freebsd	Freebsd	13.5	p7	All	All
Operating System	Freebsd	Freebsd	13.5	p8	All	All
Operating System	Freebsd	Freebsd	13.5	p9	All	All
Operating System	Freebsd	Freebsd	14.3	-	All	All
Operating System	Freebsd	Freebsd	14.3	p1	All	All
Operating System	Freebsd	Freebsd	14.3	p10	All	All
Operating System	Freebsd	Freebsd	14.3	p2	All	All
Operating System	Freebsd	Freebsd	14.3	p3	All	All
Operating System	Freebsd	Freebsd	14.3	p4	All	All
Operating System	Freebsd	Freebsd	14.3	p5	All	All
Operating System	Freebsd	Freebsd	14.3	p6	All	All
Operating System	Freebsd	Freebsd	14.3	p7	All	All
Operating System	Freebsd	Freebsd	14.3	p8	All	All
Operating System	Freebsd	Freebsd	14.3	p9	All	All
Operating System	Freebsd	Freebsd	14.4	-	All	All
Operating System	Freebsd	Freebsd	14.4	p1	All	All
Operating System	Freebsd	Freebsd	14.4	rc1	All	All
Operating System	Freebsd	Freebsd	15.0	-	All	All
Operating System	Freebsd	Freebsd	15.0	p1	All	All

Operating System	Freebsd	Freebsd	15.0	p2	All	All
Operating System	Freebsd	Freebsd	15.0	p3	All	All
Operating System	Freebsd	Freebsd	15.0	p4	All	All
Operating System	Freebsd	Freebsd	15.0	p5	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	FreeBSD	FreeBSD	affected 15.0-RELEASE p6 release	Not specified
CNA	FreeBSD	FreeBSD	affected 14.4-RELEASE p2 release	Not specified
CNA	FreeBSD	FreeBSD	affected 14.3-RELEASE p11 release	Not specified
CNA	FreeBSD	FreeBSD	affected 13.5-RELEASE p12 release	Not specified

References

Reference	Source	Link	Tags
security.freebsd.org/advisories/FreeBSD-SA-26:10.tty.asc	secteam@freebsd.org	security.freebsd.org	Vendor Advisory
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: Nicholas Carlini using Claude, Anthropic (en)

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