Remote code execution via RPCSEC_GSS packet validation

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-4747
State	PUBLISHED
Assigner	freebsd
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-26 07:16:20 UTC
Updated	2026-04-01 15:23:23 UTC
Description	Each RPCSEC_GSS data packet is validated by a routine which checks a signature in the packet. This routine copies a por

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from ADP

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

EPSS: 0.001640000 probability, percentile 0.373780000 (date 2026-04-01)

Problem Types: CWE-121 | CWE-121 CWE-121: Stack-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	FreeBSD	FreeBSD	affected 15.0-RELEASE p5 release	Not specified
CNA	FreeBSD	FreeBSD	affected 14.4-RELEASE p1 release	Not specified
CNA	FreeBSD	FreeBSD	affected 14.3-RELEASE p10 release	Not specified
CNA	FreeBSD	FreeBSD	affected 13.5-RELEASE p11 release	Not specified

References

Reference	Source	Link
github.com/califio/publications/blob/main/MADBugs/CVE-2026-4747/exploit.py	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
github.com/califio/publications/tree/main/MADBugs/CVE-2026-4747	af854a3a-2127-422b-91ae-364da2661108	github.com
security.freebsd.org/advisories/FreeBSD-SA-26:08.rpcsec_gss.asc	secteam@freebsd.org	security.freebsc
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Nicholas Carlini using Claude, Anthropic (en)

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