



OpenBao's Namespace Deletion May Not Delete Data Properly

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

Summary

CVE	CVE-2026-42186
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-14 15:16:46 UTC
Updated	2026-05-14 17:18:18 UTC
Description	OpenBao is an open source identity-based secrets management system. Prior to 2.5.3, when OpenBao's initial namespace

Risk And Classification

Primary CVSS: v4.0 2.3 LOW from security-advisories@github.com

CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000400000 probability, percentile 0.120150000 (date 2026-05-15)

Problem Types: CWE-212 | CWE-212 CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	2.3	LOW	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/S
4.0	CNA	DECLARED	2.3	LOW	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality: None
 Integrity: Low
 Availability: None
 Sub Conf.: None
 Sub Integrity: Low
 Sub Availability: None

CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Openbao	Openbao	affected < 2.5.3	Not specified

References

Reference	Source	Link	T
github.com/openbao/openbao/commit/6d2e0506e2b41be0eaa6643bf7b4efc9a2c09445	security-advisories@github.com	github.com	
github.com/openbao/openbao/releases/tag/v2.5.3	security-advisories@github.com	github.com	
github.com/openbao/openbao/security/advisories/GHSA-vv66-6rp4-wr4f	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	cc
NVD vulnerability detail	NVD	nvd.nist.gov	cc

No vendor comments have been submitted for this CVE.

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

