Sleuth Kit APFS Keybag Parser Out-of-Bounds Read

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

Summary

CVE	CVE-2026-40025
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-08 22:16:22 UTC
Updated	2026-04-08 22:16:22 UTC
Description	The Sleuth Kit through 4.14.0 contains an out-of-bounds read vulnerability in the APFS filesystem keybag parser where the

Risk And Classification

Primary CVSS: v4.0 4.8 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:L/SC:N/SI:N/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000130000 probability, percentile 0.020190000 (date 2026-04-09)

Problem Types: CWE-125 | CWE-125 CWE-125: Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:L/SC:N/SI:N/SA
4.0	CNA	CVSS	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:L/SC:N/SI:N/SA
3.1	disclosure@vulncheck.com	Primary	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:L
3.1	CNA	CVSS	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:L

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

Low

Integrity

None

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:L/SC:N/SI:N/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Sleuthkit	Sleuthkit	affected 4.14.0 custom	Not specified
CNA	Sleuthkit	Sleuthkit	unaffected 8b9c9e7d493bd68624f3b1a3963edd45c3ff7611 git	Not specified

References

Reference	Source	Link	Tags

Reference	Source	Link	Tags
github.com/sleuthkit/sleuthkit/commit/8b9c9e7d493bd68624f3b1a3963edd45c3...	disclosure@vulncheck.com	github.com	
www.vulncheck.com/advisories/sleuth-kit-apfs-keybag-parser-out-of-bounds-read	disclosure@vulncheck.com	www.vulncheck.com	
mobasi.ai/sentinel	disclosure@vulncheck.com	mobasi.ai	
github.com/sleuthkit/sleuthkit/pull/3444	disclosure@vulncheck.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

Vendor Comments And Credit

Discovery Credit

CNA: Mobasi Security Team (en)

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