



OP-TEE: PKCS#11 TA out-of-bounds read and memory disclosure

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

Summary

CVE	CVE-2026-33317
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 03:16:11 UTC
Updated	2026-04-24 03:16:11 UTC
Description	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; C

Risk And Classification

Primary CVSS: v3.1 8.7 HIGH from security-advisories@github.com

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

Problem Types: CWE-125 | CWE-787 | CWE-125 CWE-125: Out-of-bounds Read | CWE-787 CWE-787: Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	8.7	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L
3.1	CNA	DECLARED	8.7	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OP-TEE	Optee Os	affected >= 3.13.0, <= 4.10.0	Not specified

References

Reference	Source	Link
github.com/OP-TEE/optee_os/security/advisories/GHSA-8cqw-mg7v-c9p9	security-advisories@github.com	github.com
github.com/OP-TEE/optee_os/commit/e031c4e562023fd9f199e39fd2e85797e4cbdca9	security-advisories@github.com	github.com
github.com/OP-TEE/optee_os/commit/16926d5a46934c46e6656246b4fc18385a246900	security-advisories@github.com	github.com
github.com/OP-TEE/optee_os/commit/149e8d7ecc4ef8bb00ab4a37fd2ccede6d79e1ca	security-advisories@github.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report