CoCoS attested TLS is vulnerable to relay attacks via extracted ephemeral TLS keys

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-33697
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 00:16:23 UTC
Updated	2026-03-30 13:26:29 UTC
Description	Cocos AI is a confidential computing system for AI. The current implementation of attested TLS (aTLS) in CoCoS is vulnera

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from security-advisories@github.com

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

EPSS: 0.000040000 probability, percentile 0.001430000 (date 2026-04-01)

Problem Types: CWE-322 | CWE-346 | CWE-322 CWE-322: Key Exchange without Entity Authentication | CWE-346 CWE-346: Origin Validation Error

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.5	HIGH	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ultravioletrs	Cocos	affected >= 0.4.0, < 0.8.2	Not specified

References

Reference	Source	Link	Tags
github.com/ultravioletrs/cocos/security/advisories/GHSA-vfgg-mvxx-mgg7	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

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