



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

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

## Summary

<b>CVE</b>	CVE-2026-33697
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-27 00:16:23 UTC
<b>Updated</b>	2026-03-30 13:26:29 UTC
<b>Description</b>	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

Integrity

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	<a href="#">Ultravioletrs</a>	<a href="#">Cocos</a>	affected >= 0.4.0, < 0.8.2	Not specified

### References

Reference	Source	Link	Tags
<a href="https://github.com/ultravioletrs/cocos/security/advisories/GHSA-vfgg-mvxx-mgg7">github.com/ultravioletrs/cocos/security/advisories/GHSA-vfgg-mvxx-mgg7</a>	<a href="mailto:security-advisories@github.com">security-advisories@github.com</a>	<a href="https://github.com">github.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, anal

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**