

Early Attestation is Very Harmful. Why is it Required?

Muhammad Usama Sardar^{1,2} and Songbo Bu³
(ACK: Kaya Ercihan)

¹TU Dresden, Germany

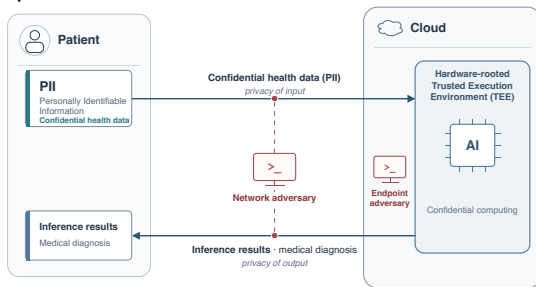
²Chair, Trusted Research Environment (TRE) Open Suite,
Global Alliance for Genomics and Health (GA4GH)

³Stevens Institute of Technology, New York, USA

October 5, 2026

Recap from LPC'25: Confidential Computing (CC)

- GA4GH example use case



- Inside TEE: **decrypt**, **compute**, and then **encrypt** results
- Attested TLS implementers, e.g., Edgeless Systems and Cocos AI
 - Edgeless Systems**: Awarded **second** place in the cybersecurity category of the WirtschaftsWoche's well-known "Best of Technology Awards"¹ (**CVE-2026-33697** and **CVE-2026-100835**)
 - Cocos AI**: Claimed as the **most** secure solution for attested TLS in CCC (**CVE-2026-33697**)

¹<https://award.wiwo.de/bot/gewinner-2026/>

Comparison with Other CC Vulnerabilities

- Much more **severe** compared to existing CVEs

Vulnerability	CVE	CWE	CVSS	Severity ²
wiretap.fail	No CVE	–	–	None
TEE.fail	No CVE	–	–	None
DDROP	No CVE	–	–	None
TDXdown	CVE-2024-27457	CWE-754	2.5	Low
Staleus	CVE-2025-54509	CWE-1262	4.0	Medium
BadRAM	CVE-2024-21944	CWE-20	5.3	Medium
BreakFAST	CVE-2025-61971	CWE-1233	5.9	Medium
Fabricked	CVE-2025-54510	CWE-414	5.9	Medium
Intra-handshake.fail ³	CVE-2026-33697	CWE-322, CWE-346	7.5	High
EarlyAttestationBleed ⁴	CVE-2026-92701	CWE-346, CWE-354	9.1	Critical
EarlyAttestationBleed	CVE-2026-92702	CWE-346	9.1	Critical
EarlyAttestationBleed	GHSA-m2qg-wrxv-h898	CWE-20	9.0–10.0	Critical
EarlyAttestationTschüss (EAT)	CVE-2026-100835	CWE-295	9.1	Critical

²Follows NIST criteria for severity <https://nvd.nist.gov/vuln-metrics/cvss>

³Intra-handshake.fail at https://www.researchgate.net/publication/408219182_Intra-handshakefail_CVE-2026-33697_High-severity_CVE_in_Attested_TLS

⁴EarlyAttestationBleed at https://www.researchgate.net/publication/414529199_EarlyAttestationBleed_Three_Critical-severity_Vulnerabilities_of_CVSS_90_in_Confidential_Computing

Root Cause and Implication of Published CVEs

CVE	Root cause	Implication
CVE-2026-33697 ⁵	Weak binder	Relay attack
CVE-2026-92701 ⁶	TDX REPORT_DATA comparison missing	Local application-data release
CVE-2026-92702	SNP zero-length input check missing	Fail-open lower verifier API
CVE-2026-100833	Image-digest policy bypass	Unauthorized image accepted
CVE-2026-100835 ⁷	Machine ID check missing	Wrong physical host trusted

- **Confidentiality**: complete data leak
- **Integrity**: complete data modification
- Globally unique machine identifiers for machine; otherwise, it could be any machine in the world
- Who will provide such reference identifiers?

⁵Intra-handshake.fail at https://www.researchgate.net/publication/408219182_Intra-handshakefail_CVE-2026-33697_High-severity_CVE_in_Attested_TLS

⁶EarlyAttestationBleed at https://www.researchgate.net/publication/414529199_EarlyAttestationBleed_Three_Critical-severity_Vulnerabilities_of_CVSS_90_in_Confidential_Computing

⁷EarlyAttestationTschüss (EAT)

Early Attestation Tschüss (EAT)

- **Edgeless Systems Contrast** and **draft-fossati-seat-early-attestation-07** are still vulnerable in our analysis.

Affected Component	Archived	Migrated	Withdrawn	Still Vulnerable
CCC Attestation SIG reference implementation	Yes			
Cocos AI $\leq$ v0.8.2		Yes		
Privasys rustls $\leq$ v0.2.0	Yes	Yes		
Privasys Go $\leq$ v0.3.0-go1.26.5	Yes	Yes		
draft-fossati-tls-attestation-10			Yes	
draft-ritz-seat-facts-00	Yes			
Edgeless Systems Contrast				Follows withdrawn draft
draft-fossati-seat-early-attestation-07				Yes

Published Status⁸ on Early Attestation

Responsible Disclosures for all 37 GHSAs and 5 CVEs

CVSS	Severity	Number of Published GHSAs	Number of Published CVEs
9.0–10.0	Critical	2	—
9.8	Critical	1	—
9.1	Critical	8	3
8.2	High	1	1
7.8	High	2	—
7.7	High	2	—
7.6	High	1	—
7.5	High	3	1
7.4	High	4	—
6.5	Medium	3	—
6.3	Medium	3	—
5.5	Medium	1	—
5.3	Medium	1	—
4.4	Medium	1	—
4.3	Medium	1	—
4.2	Medium	1	—
3.7	Low	1	—

⁸estimated as of 04.10.2026, <https://www.ietf.org/archive/id/draft-intra-handshake-fail-55.html#section-1.1>

Early Attestation in the News

SECURITY

Confidential computing's trust mechanism is broken. The fix may not exist

Attested TLS: the handshake that can't prove who's on the other end

CVE-2026-92702: Critical vulnerability in Cocos AI up to version 0.8.2 fixed

September 21, 2026 | Weaknesses

The core of the trust mechanism in confidential computing has broken down—and may be irreparable.

Attested TLS Was Supposed to Be the Last Trust Boundary. It Isn't.

by Sal Kimmich · July 12th, 2026

TLDR >

EN RU ES JA TA LV TH LT MN NL UK SQ

ATTESTED TLS WAS SUPPOSED TO BE THE LAST TRUST BOUNDARY.

CVE-2026-33697: Attested TLS Relay Flaw Hits WhatsApp, Cocos AI

CVE-2026-33697 lets relay attacks redirect confidential computing traffic without breaking attestation, affecting WhatsApp, Cocos AI, and Edgeless Systems.

Cloud Security

Confidential computing's remote attestation protocol may have fundamental flaw

Attested TLS Vulnerability Exposes Secure Cloud Data

BY NAM PHONG · PUBLISHED JULY 8, 2026 · UPDATED JULY 8, 2026

Critical Flaw Discovered in Confidential Computing Attestation Protocols

Early evidence may expose confidential data to high risk

Safety 114  Updated September 22

CVE-2026-92701: Critical vulnerability in Trusted Execution Environments up to version 0.8.2

September 22, 2026 | Weaknesses

More CVEs⁹ (yet to be published) on Early Attestation

CVSS	Severity	Number of CVEs
9.0–10.0	Critical	3
9.8	Critical	2
9.1	Critical	5
8.7	High	1
7.8	High	3
7.7	High	2
7.6	High	1
7.5	High	6
7.4	High	13
6.5	Medium	10
6.3	Medium	10
5.5	Medium	1
5.3	Medium	1
4.4	Medium	1
4.3	Medium	1
4.2	Medium	1
3.7	Low	1

⁹estimated as of 04.10.2026, <https://www.ietf.org/archive/id/draft-intra-handshake-fail-55.html#section-8>

Discussion: Architectural Problems of Early Attestation

- **Hardware-level** information of server
 1. Malicious client gets Evidence **before** the server has authenticated the client
 2. Client may exploit weaknesses (e.g., vulnerable firmware version)
- **Only Boot-time Claims**
 - Runtime Claims are not available at the handshake time
- Re-attestation
 - Claims typically change over time, e.g., **dynamic** workloads and **long-lived** connections.
 - **Critical kernel data structures** may change after boot.
 - Early attestation assumes static Evidence.
- **Unnecessary Complexity**
 - Protocol bloat
- High Handshake **Latency and Timeouts**
 - Appraisal typically involves remote calls
- Binding to **application traffic secrets** (CVE-2026-33697)
 - Evidence is generated before the application traffic keys even exist

Which security or privacy property
Early Attestation can achieve that
standard attestation cannot?

Too many vulnerabilities in Early
Attestation; we need your **help**!

Links to Resources

- Internet-Draft (contributors and co-authors very welcome!)
 - <https://datatracker.ietf.org/doc/draft-intra-handshake-fail/>
- EarlyAttestationBleed pre-print
 - https://www.researchgate.net/publication/414529199_EarlyAttestationBleed_Three_Critical-severity_Vulnerabilities_of_CVSS_90_in_Confidential_Computing
- EarlyAttestationTschüss coming soon

ACK: Co-authors (in papers/IETF drafts)

- Viacheslav Dubeyko (CoreWeave)
- Jean-Marie Jacquet (University of Namur)
- Songbo Bu (Stevens Institute of Technology)
- Chengxin Huang (Independent)
- Haowen Song (Shanghai Guan An Information Technology Co., Ltd.)
- Kaya Ercihan (Switch)
- Kubilay Ahmet Küçük (DPhil Oxford University)
- Sylvain Bellemare (Sureshot Labs)
- Eva C. M. Willems (Independent)
- Justin DESSENNES SAINTEN (Independent Corporate Risk Consultant)
- Massimiliano Brighindi (PHI-OMEGA)
- Mikerah Quintyne-Collins (HashCloak Inc and Stoffel Labs Inc)
- Iman Schrock (EMILIA Protocol, Inc.)
- Ammara Gul (Birmingham City University)
- Serhii Nikolaichuk (The Capital Index, Austin, Texas)
- Ionut Mihalcea (Arm)
- Thomas Fossati (Nvidia)
- Arto Niemi (Huawei)
- Hannes Tschofenig (Universität der Bundeswehr München)
- Simon Frost (Arm)
- Ned Smith (Intel)
- Carsten Weinhold (Barkhausen Institut)
- Michael Roitzsch (Barkhausen Institut)
- Yogesh Deshpande (Arm)
- Yaron Sheffer (Intuit)
- Tirumaleswar Reddy K. (Nokia)
- Henk Birkholz (Fraunhofer SIT)
- Mariam Moustafa (Aalto University)
- Tuomas Aura (Aalto University)
- Liang Xia (Huawei)
- Weiyu Jiang (Huawei)
- Jun Zhang (Huawei)
- Houda Labiod (Huawei)
- Yuning Jiang (Huawei International)
- Meiling Chen (China Mobile)
- Minghui Xu (Shandong University)
- Pavel Nikonorov (GENXT)
- Camilo A. Posada (ULISSY s.r.l.)
- and many others...

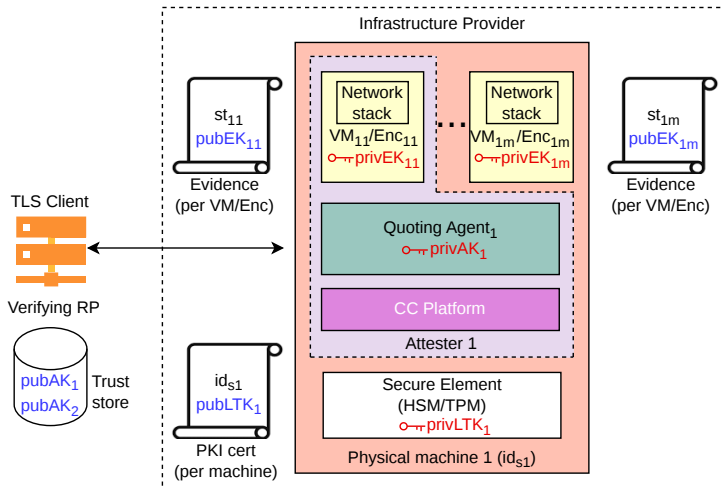
ACK: Contributors

- Eric Rescorla (Independent)
- Laurence Lundblade (Security Theory LLC)
- Göran Selander (Ericsson AB)
- Marco Tiloca (RISE AB)
- Richard Barnes (Cloudflare)
- Giridhar Mandyam (AMD)
- Christopher Patton (Cloudflare)
- Dionna Amalie Glaze (Google)
- Bob Beck (Google)
- Mike Ounsworth (Cryptic Forest Software)
- John Preuß Mattsson (Ericsson Research)
- Cedric Fournet (Microsoft)
- Thore Sommer (TU Munich)
- Nikolaus Thümmel (Scontain)
- Jonathan Hoyland (Cloudflare)
- Jo Van Bulck (KU Leuven)
- Martin Thomson (Mozilla)
- Britta Hale (Naval Postgraduate School)
- Werner Staub (CORE Association)
- Christian Simmen (DENIC)
- Dennis Jackson (Mozilla)
- Peg Jones (Flashbots)
- Paul Wouters (Aiven)
- Matthias Wählisch (TU Dresden)

- Andrey Ruzhanskiy (Telekom MMS)
- Muuhh Ikede (Cybertrust)
- Mike Bursell (CCC)
- Ravi Sahita (Rivos)
- Samuel Ortiz (Rivos)
- Mathieu Poirier (Linaro)
- Hannes Reinecke (SUSE)
- Alexander Graf (AWS)
- Elena Reshetova (Intel)
- Jon Lange (Microsoft)
- Daniel Kiper
- David Woodhouse (AWS)
- David Kaplan (AMD)
- Tiziano Santoro (Google)
- Juho Forsén
- Ira McDonald
- Markus Rudy (Edgeless Systems)
- Ayoub Benaissa (Zama)
- Greg Kostal (Microsoft)
- Mike Stunes (Microsoft)
- David Altobelli (Microsoft)
- Venkat Malladi (Quest Diagnostics)
- Tom Conner (Broad Institute of MIT and Harvard)
- Jaime Delgado (Universitat Politècnica de Catalunya)

System and Threat Model

- Confidential Computing Consortium (CCC) threat model:
Infrastructure provider (compute provider) is untrusted



EarlyAttestationBleed¹³

- Cocos AI
 - **Attack1**: comparison with expected input value missing
 - CVE-2026-92701¹⁰ of CVSS **9.1 (CRITICAL)**
 - **Attack2**: comparison is correct but bypassed for zero-length input
 - CVE-2026-92702¹¹ of CVSS **9.1 (CRITICAL)**
 - Cocos AI migrated to standard (post-handshake) attestation
- Edgeless Systems
 - **Attack3**: Authorization predicate accepts without selecting an applicable policy entry
 - Published Security Advisory¹² with **CRITICAL** severity (**9.0-10.0**)

¹⁰<https://www.cve.org/CVERecord?id=CVE-2026-92701>

¹¹<https://www.cve.org/CVERecord?id=CVE-2026-92702>

¹²<https://github.com/edgelessssys/contrast/security/advisories/GHSA-m2qg-wrxv-h898>

¹³https://www.researchgate.net/publication/414529199_EarlyAttestationBleed_Three_Critical-severity_Vulnerabilities_of_CVSS_90_in_Confidential_Computing