EarlyAttestationBleed and EarlyAttestationTschüss (EAT)

Muhammad Usama Sardar[1,2] and Songbo Bu[3]

ACK: Bertrand Foing [Privasys owner], Markus Rudy [Edgeless Systems Contrast maintainer], Sammy Kerata Oina [Cocos AI maintainer], Kaya Ercihan [Switch], David Kaplan [AMD], Elena Reshetova [Intel], Artem Bityutskiy [Intel], Mateusz Bronk [Intel], and Kubilay Ahmet Küçük [Oxford University D.Phil. Ph.D. Alum]

[1]Technical University of Dresden, Dresden, Germany
[2]Chair, Trusted Research Environment (TRE) Open Suite,
Global Alliance for Genomics and Health (GA4GH), Toronto, Canada
[3]Stevens Institute of Technology, New York, USA

November 16, 2026

Problem: German Community is at Critical Risk

Health data of 50 million[1] insured Germans using AOK, Barmer, and Techniker Krankenkasse (TK), potentially at critical risk because of vulnerable early attestation protocols

[1] https://web.archive.org/web/20261115124637/https://www.edgeless.systems/resource-library/epa

Problem Context

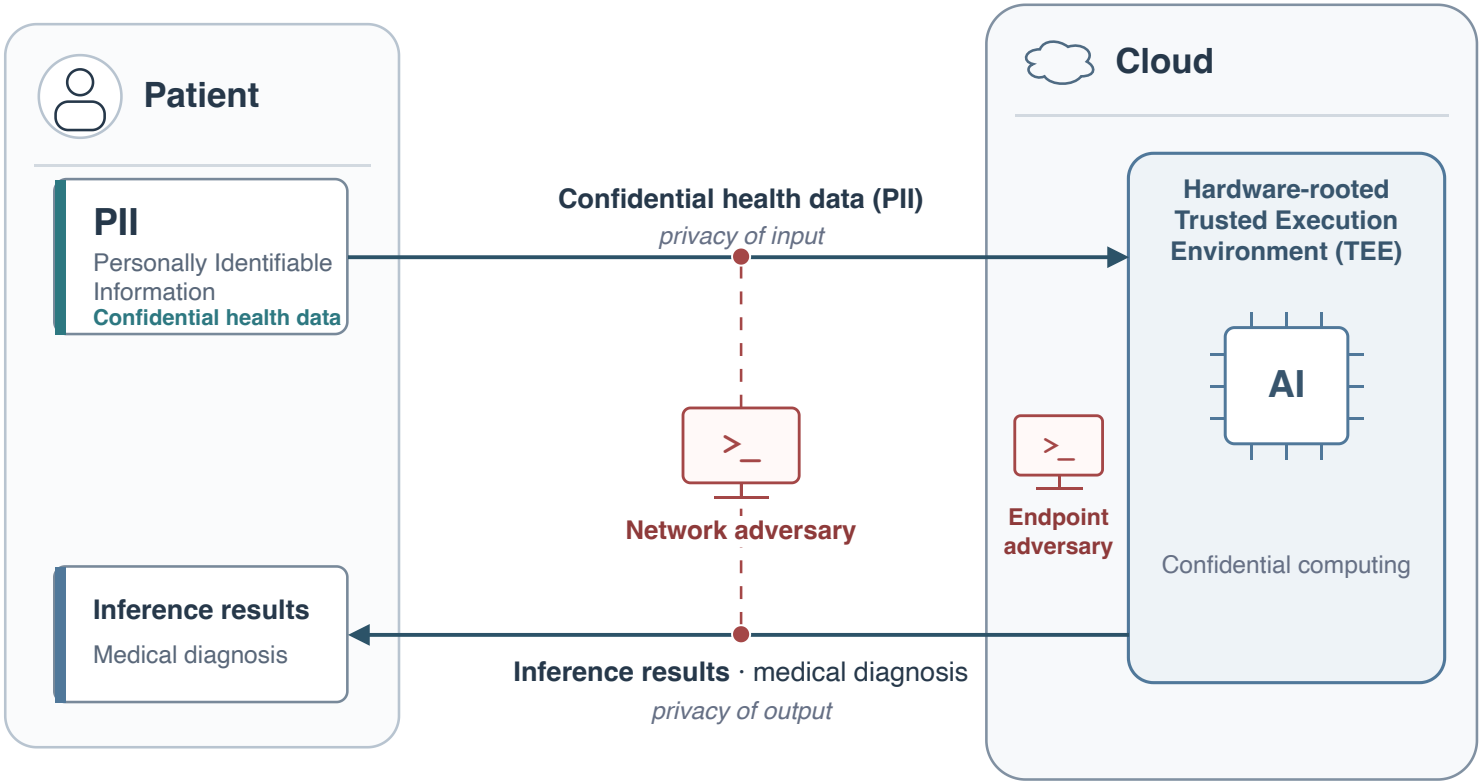
Electronic health record "Elektronische Patientenakte (ePA)"[2] by Edgeless Systems software.

[2] https://web.archive.org/web/20261115124637/https://www.edgeless.systems/resource-library/epa

Centralized computation in the cloud

- Single point of failure/trust
- Service provider TCB lock-in for reference machine IDs
- Cloud provider TCB lock-in
- Hardware provider TCB lock-in

GA4GH Example Use Case of Confidential Computing



- Inside TEE: decrypt, compute, and then encrypt results
- Attested secure connection, e.g., attested TLS

Early vs. Standard Attestation for TLS 1.3

- Early (intra-handshake) attestation: draft-fossati-seat-early-attestation
- Standard (post-handshake) attestation: RFC9261

Vulnerabilities in Early Attestation Ecosystem

- 39 GHSAs published
  - Critical: 13
  - High: 14
  - Medium: 11
  - Low: 1
- 20 CVEs published
  - Critical: 14
  - High: 6
- 57+ more CVEs in process
  - Critical: 5
  - High: 26
  - Medium: 25
  - Low: 1

Comparison with Other Related Vulnerabilities

- Much more severe compared to existing CVEs

Vulnerability	CVE	CWE	CVSS	Severity[3]
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[4]	CVE-2026-33697	CWE-322, CWE-346	7.5	High
EarlyAttestationBleed[5]	CVE-2026-92701	CWE-346, CWE-354	9.1	Critical
EarlyAttestationBleed	CVE-2026-92702	CWE-346	9.1	Critical
EarlyAttestationBleed	CVE-2026-100833	CWE-20	9.6	Critical
EarlyAttestationTschüss (EAT)	CVE-2026-100835	CWE-295	9.1	Critical
EarlyAttestationTschüss (EAT)	CVE-2026-112377	CWE-346	9.1	Critical
EarlyAttestationTschüss (EAT)	CVE-2026-108362	CWE-346	9.1	Critical
EarlyAttestationTschüss (EAT)	CVE-2026-108265 till -9	CWE-346	9.1	Critical
EarlyAttestationTschüss (EAT)	CVE-2026-119344	CWE-346	9.1	Critical

[3] Follows NIST criteria for severity https://nvd.nist.gov/vuln-metrics/cvss

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

[5] EarlyAttestationBleed at https://www.researchgate.net/publication/414529199_EarlyAttestationBleed_Three_Critical-severity_Vulnerabilities_of_CVSS_90_in_Confidential_Computing

Root Cause and Implication of Selected Published CVEs

CVE	Root cause	Implication
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-2026-108265[7]	No connection binding	Relay attack
CVE-2026-100835	No hardware (machine ID) binding	Wrong physical host trusted

- Highlighted vulnerabilities
  - CVE-2026-108265: No binding to connection ⇒ Relay attacks
  - CVE-2026-100835: No binding to hardware ⇒ Diversion attacks
- Who will provide such reference machine IDs?
  - Edgeless Systems itself provides the reference machine IDs for Privatemode ⇒ Edgeless Systems remains within the TCB.

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

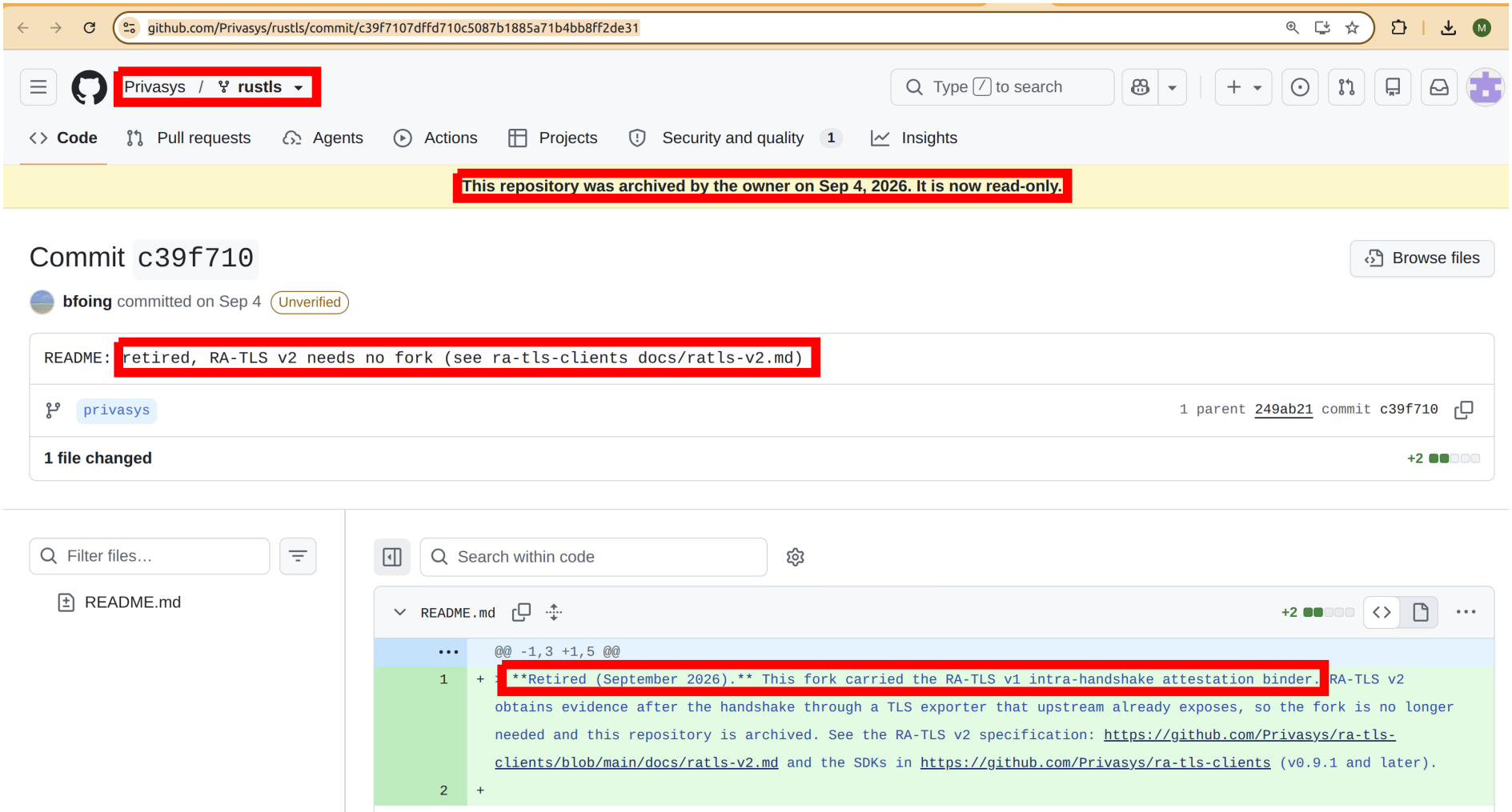
[7] `https://www.researchgate.net/publication/417343302_EarlyAttestationTschuss_EAT`

EarlyAttestationTschüss (EAT): End of Life

Affected Component	Archived	Migrated	Withdrawn	Still Vulnerable
Privasys rustls $\leq$ v0.2.0	**Yes**	**Yes**		
Privasys Go $\leq$ v0.3.0-go1.26.5	**Yes**	**Yes**		
Cocos AI $\leq$ v0.8.2		**Yes**		
CCC Attestation SIG reference implementation	**Yes**			
draft-fossati-tls-attestation-10			**Yes**	
Edgeless Systems Contrast				**Follows withdrawn draft**
Meta Private Processing				**Follows withdrawn draft**
draft-fossati-seat-early-attestation-09				**No shared secrets in binder**

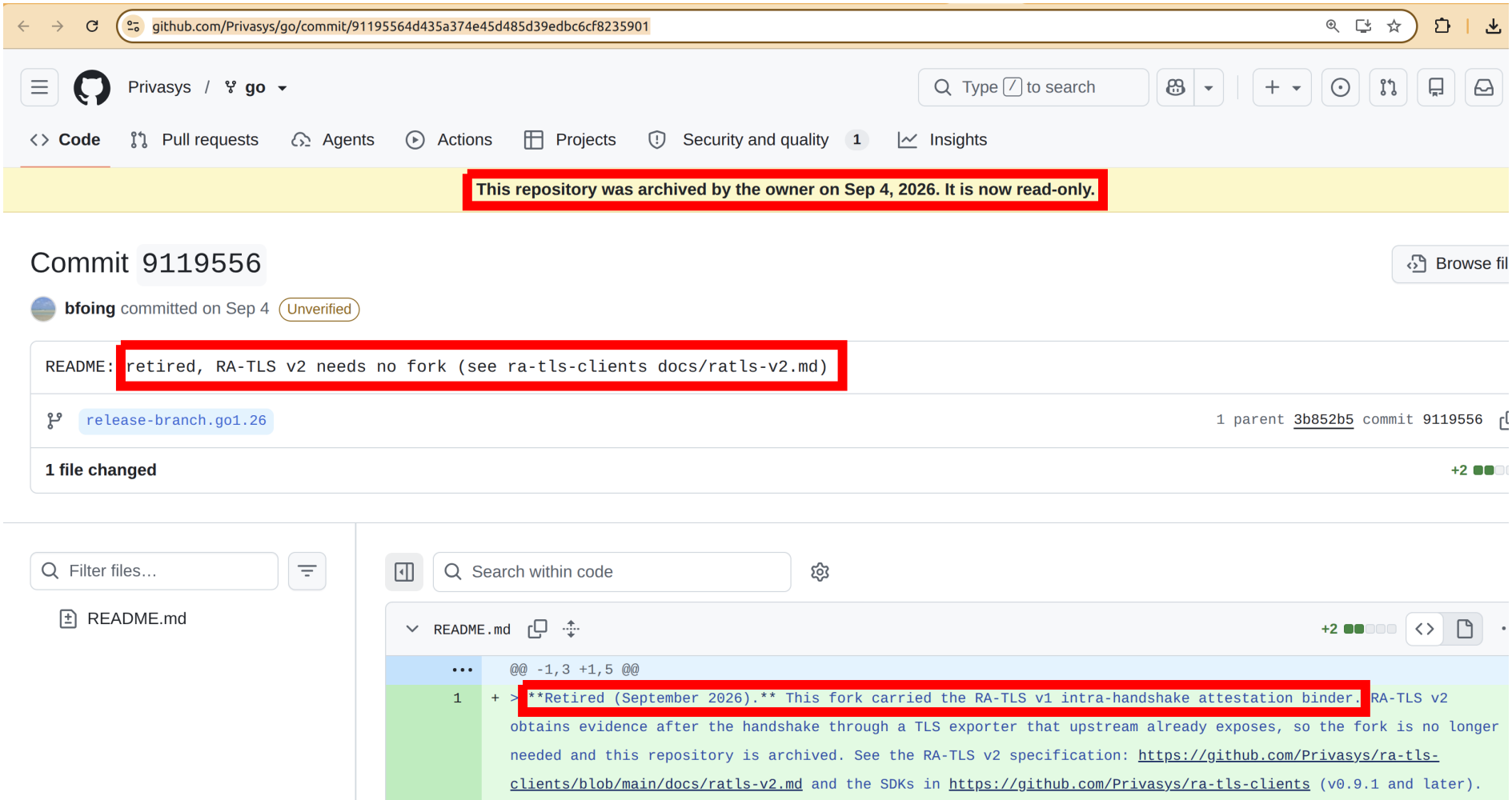
- Edgeless Systems Contrast and Meta following the withdrawn draft.
- draft-fossati-seat-early-attestation-09 is still vulnerable in our analysis.

End of Life of Early Attestation in Privasys rustls[8]



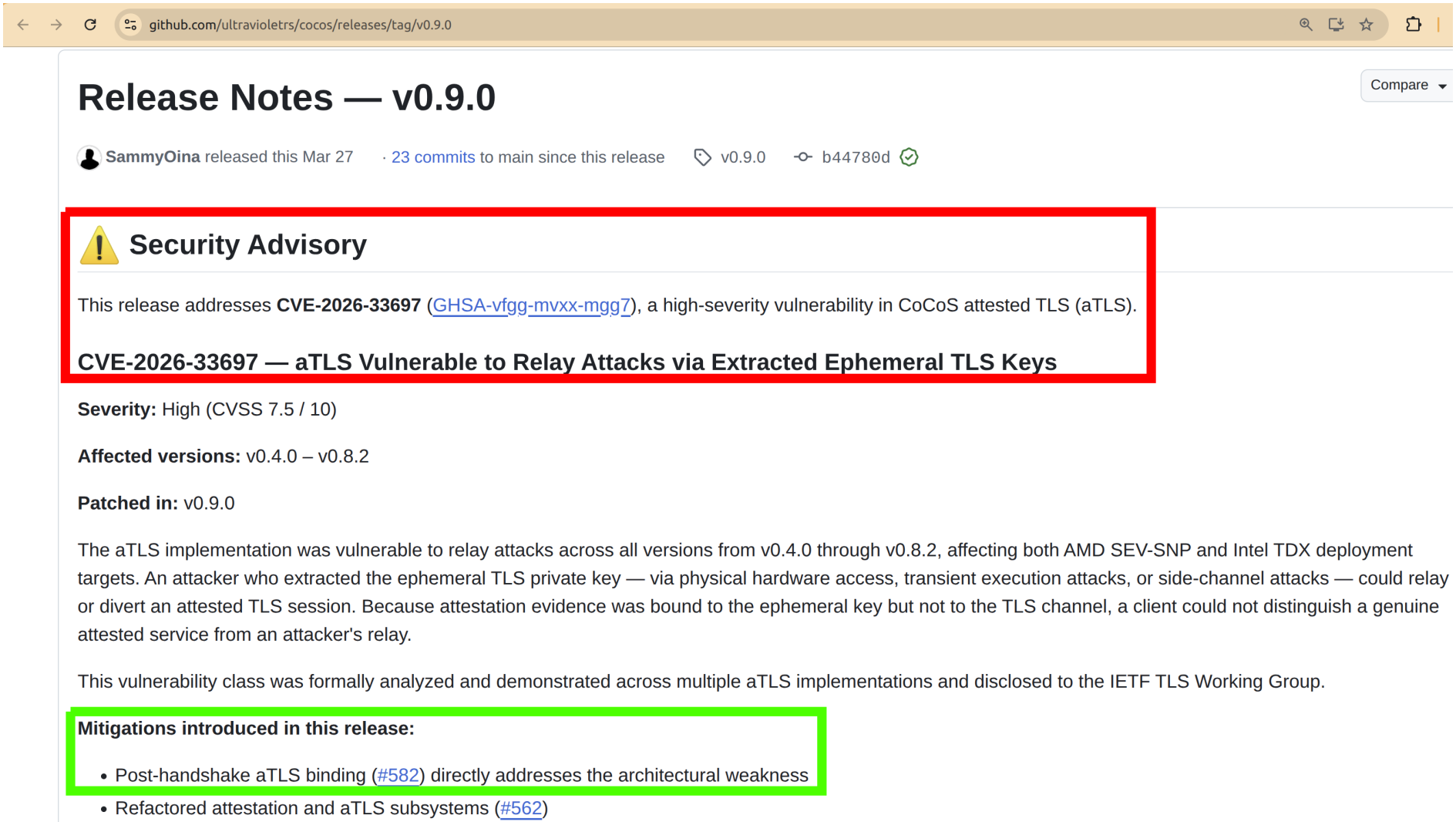
[8] https://github.com/Privasys/rustls/commit/c39f7107dffd710c5087b1885a71b4bb8ff2de31

End of Life of Early Attestation in Privasys Go[9]



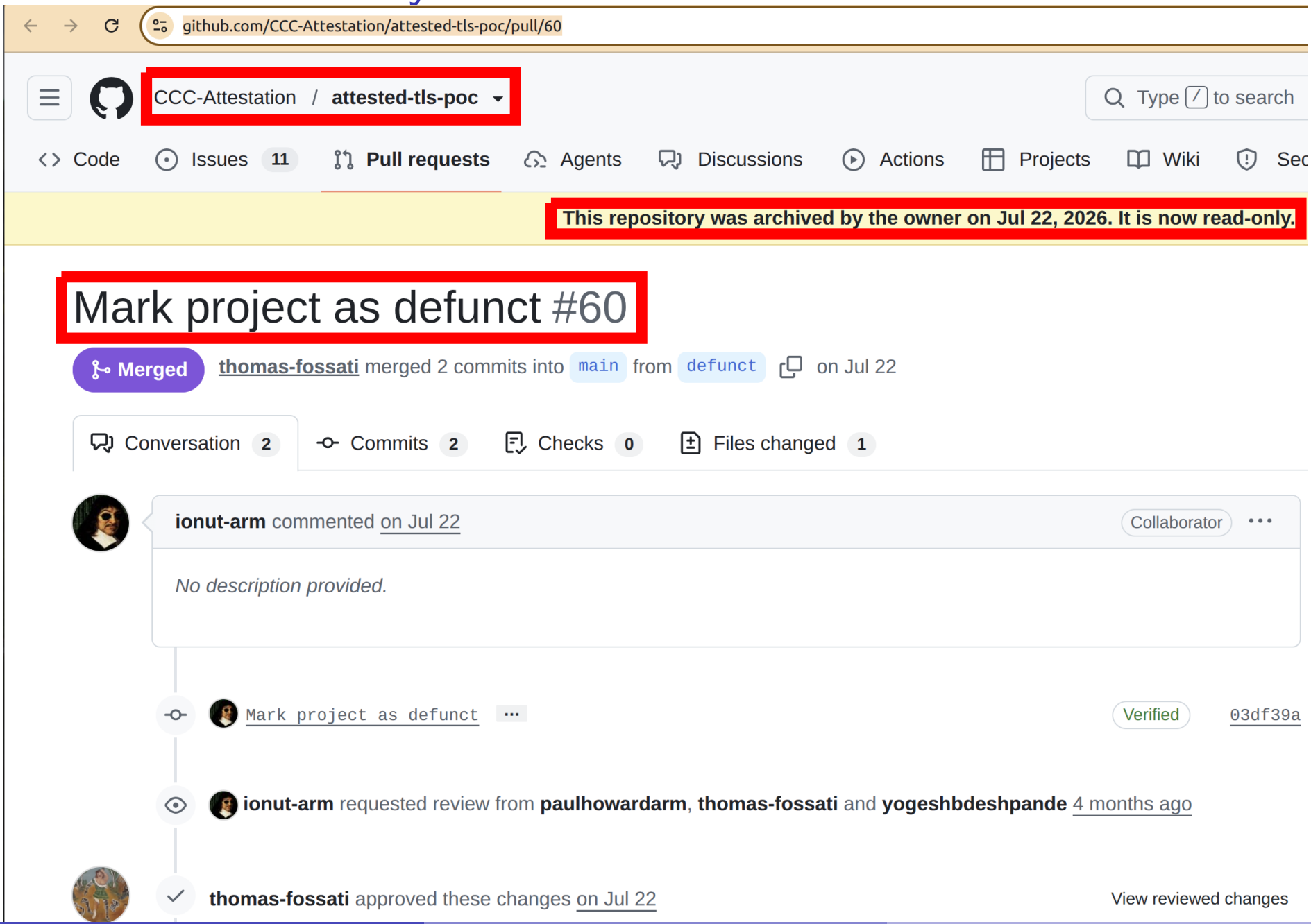
[9] https://github.com/Privasys/go/commit/91195564d435a374e45d485d39edbc6cf8235901

End of Life of Early Attestation in Cocos AI[10]

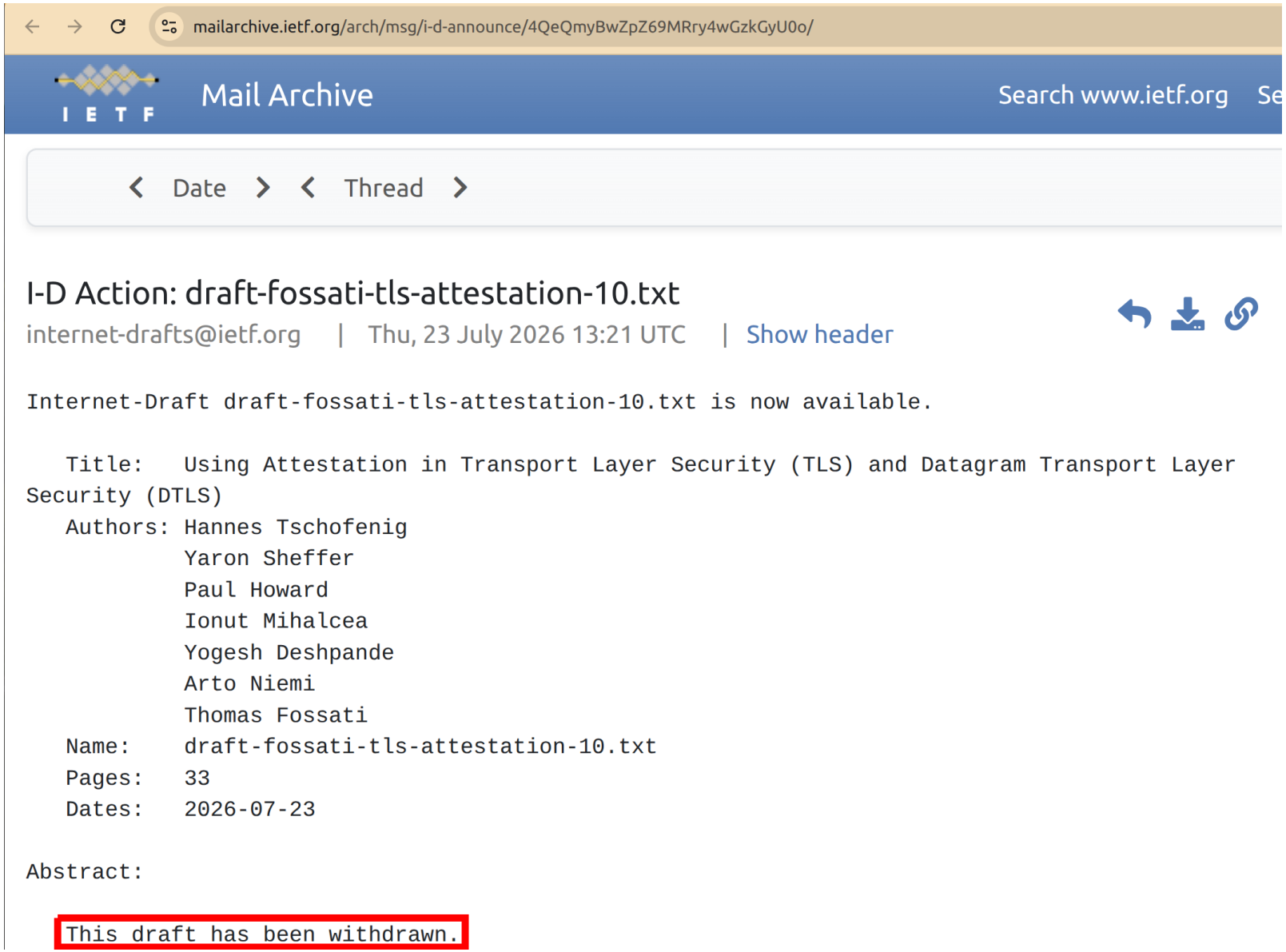


[10] https://github.com/ultravioletrs/cocos/releases/tag/v0.9.0

End of Life of Early Attestation in CCC Attestation SIG[11]



End of Life of draft-fossati-tls-attestation[12]



[12] https://mailarchive.ietf.org/arch/msg/i-d-announce/4QeQmyBwZpZ69MRry4wGzkGyU0o/

Acknowledgment of Vulnerabilities of Early Attestation[13]

- Repo owners and maintainers: accepted GHSAs and requested CVEs
- GitHub and VulnCheck (as CNA)
- NIST
- ENISA
- China Information Technology Security Evaluation Center (CNITSEC)
- Many other reputable international vulnerability database managers
- Global Alliance for Genomics and Health (GA4GH)
- IRTF UFMRG
- IRTF CFRG
- Confidential Computing Consortium (CCC)
- Agentic AI Foundation (AAIF)
- Open Compute Project (OCP) security
- Linux Plumbers Conference (LPC)
- RIPE
- Many others

[13] see authentic references at `https://mailarchive.ietf.org/arch/msg/cfrg/_Ol3Ft4PZFrg47Nujxr_xvRgoq4/`

Published Status[14] on Early Attestation

Responsible Disclosures for all 39 GHSAs and 20 CVEs

CVSS	Severity	Number of Published GHSAs	Number of Published CVEs
9.0–10.0	Critical	2	—
9.8	Critical	1	—
9.6	Critical	—	1
9.1	Critical	10	13
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	—
7.2	High	1	2
7.0	High	—	2
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	—

[14] estimated as of 16.11.2026, `https://www.ietf.org/archive/id/draft-intra-handshake-fail-62.html#section-1.1`

Active Exploitation of Early Attestation[15]

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

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

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

Critical Flaw Discovered in Confidential Computing Attestation Protocols

Early evidence may expose confidential data to high risk

Safety 114 LV8

Updated September 22

Attested TLS Was Supposed to Be the Last Trust Boundary. It Isn't. Formal Methods Show How.

by **Sal Kimmich** · July 12th, 2026

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

September 22, 2026 | Weaknesses

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.

[15] https://www.ietf.org/archive/id/draft-intra-handshake-fail-62.html#name-media-coverage

57+ CVEs[16] (yet to be published) on Early Attestation

Expected 5 critical, 26 high, 25 medium and 1 low

CVSS	Severity	Number of CVEs
9.0–10.0	Critical	3
9.8	Critical	2
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

[16] estimated as of 16.11.2026, `https://www.ietf.org/archive/id/draft-intra-handshake-fail-62.html#section-8`

Request for Discussion

Decentralize using federated learning? How to remove vendor lock-in?

Any other early attestation implementation?

Links to Resources

- Internet-Draft (contributors and co-authors very welcome!)
  - https://datatracker.ietf.org/doc/draft-intra-handshake-fail/
- EarlyAttestationBleed
  - https://www.researchgate.net/publication/414529199_EarlyAttestationBleed_Three_Critical-severity_Vulnerabilities_of_CVSS_90_in_Confidential_Computing
- EarlyAttestationTschüss
  - https://www.researchgate.net/publication/417343302_EarlyAttestationTschuss_EAT
- Identity Crisis
  - https://dl.acm.org/doi/10.1145/3779208.3785387
- Intra-handshake.fail
  - https://link.springer.com/chapter/10.1007/978-3-032-38692-2_6

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.)
- Venkat Malladi (Quest Diagnostics)
- 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)
- Tom Conner (Broad Institute of MIT and Harvard)
- Jaime Delgado (Universitat Politecnica de Catalunya)
- Yanping Hu (TU Dresden)

ACK: Contributors (continued)

- Ilari Liusvaara
- Vladislav Kostitsyn (Alakris)
- Kevin Hammond (Ensurable Systems)
- Waqas Nawaz (Vision4d)
- Kayode Oluwole Elekula
- and many others...