Audited did not mean covered.

A media evidence brief on the scope and age of audits behind H1 2026 losses.

94.4%

of losses at audited victims came from incidents outside the identified audits' scope.

135	$939.86M	68
COUNTED INCIDENTS	ESTIMATED LOSSES	AUDITED VICTIMS

WINDOW 2026-01-01 TO 2026-06-29

DATASET V1.0 / GENERATED 2026-07-01

Interactive report and dataset: ack3.ai/research/defi-hacks-h1-2026/

01 / KEY FINDINGS

Audit status is not audit coverage.

The binary label “audited” says a project was reviewed at some point. It does not establish that the eventual attack path, the live deployment or the system around the contracts was covered.

46 / 68
OUTSIDE IDENTIFIED SCOPE

20 / 68
INSIDE AUDIT SCOPE

2 / 68
SCOPE EVIDENCE INSUFFICIENT

THE OPERATING PRINCIPLE

An audit is a timestamp and a boundary, not a lifetime warranty.

Coverage finding. 46 of 68 audited victims had only out-of-scope evidence. Those incidents account for $680.97 million, or 94.4% of all losses at audited victims.

Age finding. Of the 20 incidents with an in-scope match, 17 followed the closest relevant audit by at least six months. Only three followed an audit completed less than six months earlier.

How to read it. Audit status measures project history; scope grading measures attack-path coverage. Audit age is a warning signal, not evidence that time alone caused an exploit.

02 / INCIDENT UNIVERSE

135 verified incidents. $939.86M lost.

ack3

Audit status across 135 verified incidents.

68	35	32
AUDITED	UNAUDITED	UNKNOWN

SOURCE / ack3 / DATASET V1.0

Of the 135 incidents, 68 affected projects with identified prior audit history, 35 were classified unaudited and 32 had audit status unknown. Audit status describes project history; it does not show whether the exploited path was included in a review.

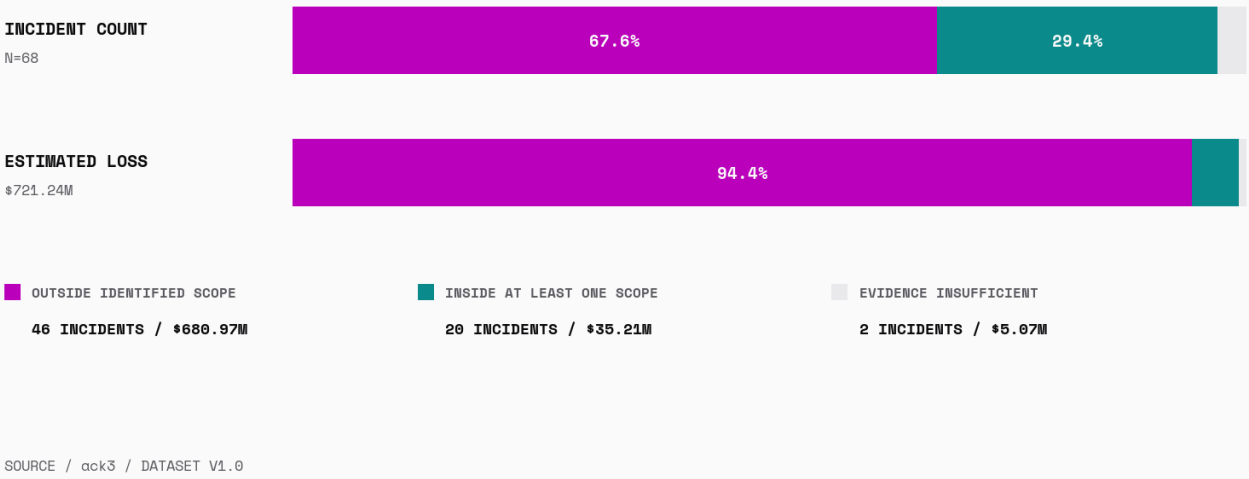
Base: 135 confirmed or likely incidents from 2026-01-01 through 2026-06-29, each supported by at least two independent sources. Losses sum the best public estimate available at the dataset cutoff. Audit status is classified from public evidence available for each affected project.

03 / AUDIT COVERAGE

Most audited-victim losses crossed the audit boundary.

ack3

Audit scope by incident count and loss.



SOURCE / ack3 / DATASET V1.0

The count and loss denominators tell different stories. Outside-scope incidents represent 67.6% of audited victims but 94.4% of audited-victim losses. Inside-scope incidents represent 29.4% by count and 4.9% by loss.

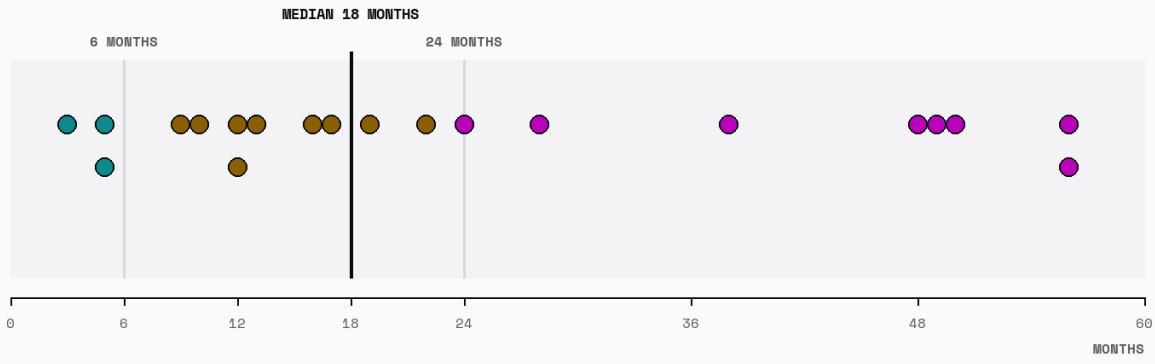
Base: 68 audited victims representing $721.24 million in losses. An incident is counted inside scope when at least one identified audit covered the exploited component; outside scope means all available scope evidence placed that component outside the identified reviews.

04 / AUDIT AGE

Point-in-time assurance aged.

ack3

Audit age distribution.



3	9	8	3-56
15%	45%	40%	
<6 MONTHS	6 TO <24 MONTHS	24+ MONTHS	OBSERVED RANGE

SOURCE / ack3 / DATASET V1.0

The 20 observed gaps range from 3 to 56 months, with a median of 18 months. Three incidents followed the closest relevant audit by less than six months; nine followed after six to under 24 months; eight followed after at least 24 months.

Age is measured at calendar-month granularity from the closest relevant pre-incident audit. It is descriptive, not causal. Post-review code changes create new, out-of-scope code; for unchanged reviewed code, the gap records how long the assurance remained in use while its surrounding system and attacker techniques evolved.

05 / THREE BOUNDARY CASES

The attack path was the system, not one repository.

Taiko Bridge

$1.70M / 2026-06-22

PUBLIC SIGNING KEY + UNCHECKED DEBUG FLAG

Taiko's postmortem identifies two conditions: an enclave signing key committed to the public Raiko repository and an attestation check that did not reject debug-mode enclaves. OpenZeppelin's 2024 scope listed Bridge.sol, SignalService.sol, ERC20Vault.sol and SgxVerifier.sol, but no Raiko repository code.

PRIMARY EVIDENCE / TAIKO POSTMORTEM + OPENZEPPELIN TAIKO AUDIT

Polymarket front end

$3.10M / 2026-06-25

THIRD-PARTY VENDOR TO USER FRONT END

Polymarket said a third-party vendor was compromised and injected a malicious script into its front end for some users. Its official contract-security repository lists reviews of deployed Polygon contracts; the compromised front-end dependency is not among those published contract scopes.

PRIMARY EVIDENCE / POLYMARKET STATEMENT + CONTRACT-SECURITY REPOSITORY

Resolv / USR

$24.50M / 2026-03-22

INFRASTRUCTURE CREDENTIAL TO ON-CHAIN MINT

Resolv's postmortem traces the attack from an upstream credential compromise, through GitHub and cloud infrastructure, to signing authority used by the Counter contract. Pashov's December 2024 review explicitly listed TheCounter.sol; its published scope was the five Solidity files named in the report.

PRIMARY EVIDENCE / RESOLV POSTMORTEM + PASHOV DECEMBER 2024 REVIEW

06 / READING THE FINDINGS

Assurance follows systems, change and attack paths.

01 The system is larger than its contracts

Published audit scopes name specific files and versions. Production risk also lives in services, keys, roles, front ends, dependencies, deployments and configuration.

02 Change creates a new assurance question

New code is outside an earlier review by definition. New dependencies, privileges, integrations and configurations can also change how reviewed code behaves in the live system.

03 Attack paths cross boundaries

Taiko, Polymarket and Resolv each connect an off-chain event to on-chain consequences. Separate component reviews can leave the relationship between them under-tested.

04 AI changes the scale of search

AI can help attackers and defenders inspect more code and more relationships. Its defensive value comes from broad machine search combined with human validation, fuzzing and threat modeling.

HOW ack3 APPLIES THIS

The H1 dataset does not attribute any incident to AI. It does show why wider system coverage matters. The ack3 AI scan runs alongside manual review to trace dependencies, integrations and boundaries beyond a contract directory; security engineers validate each result for reproducibility, exploitability and impact.

HUMAN-LED REVIEW / AI-ASSISTED COVERAGE / EVIDENCE-BACKED FINDINGS

07 / FULL RESOURCES

Full report, source data and press materials.

REPORT

Interactive report

Search the full incident table and open incident-level evidence.

ack3.ai/research/defi-hacks-h1-2026/

DATA

Source dataset

Download the versioned JSON behind every figure and table.

ack3.ai/.../defi-hacks-h1-2026/dataset.json

PRESS

Media kit

Download charts, source notes, fact sheet and press materials.

ack3.ai/.../ack3-h1-2026-media-kit.zip

CORRECTIONS

Contact the research team

Send supporting evidence, corrections or media questions.

hello@ack3.ai

LIMITS AND INTERPRETATION

PUBLIC EVIDENCE	Audit status and scope reflect evidence available at the cutoff. Unknown does not mean unaudited.
LOSS ESTIMATES	Values use the best public estimate found and may change as projects publish updates.
SCOPE	Outside identified scope describes the evidence located; it is not a score for the project or auditor.
AGE + AI	Audit age is descriptive, not causal. The dataset does not attribute any incident to AI.

SUGGESTED CITATION

ack3. DeFi Hacks H1 2026: Audited Did Not Mean Covered.
Dataset version 1.0. ACK3 LTD, 2026.