CRED SHIELDS

STATE OF WEB3 SECURITY

H1 2025

CREDSHIELDS TECHNOLOGIES PTE. LTD.

20A Tanjong Pagar Road, Singapore - 088443

State of Web3 Security – H1 2025

Introduction

Web3 security faced a turbulent start in 2025, as over 50 large-scale exploits rocked the ecosystem, driving losses beyond $2.5 billion in just six months.
From multi-billion-dollar centralized exchange breaches to rug pulls and sophisticated social engineering attacks, the period reflects how attackers continue to evolve and exploit complex vulnerabilities across chains.

This report, powered by CredShields' Web3HackHub, combines real-time exploit data, over 2.5 million SolidityScan security scans, and manual audit insights to provide:

- A global snapshot of hacked funds, incidents, and trends.
- The Top 10 Hacks of H1 2025 with root cause analysis.
- Chain-wise and category-wise impact distribution.
- A roadmap for improving Web3 security resilience.

Executive Summary

H1 2025 unfolded as one of the most volatile periods for Web3, with 56 major breaches inflicting $2.72 billion in damages across centralized and decentralized platforms. The most devastating incident was the $1.45 billion Bybit exploit, where attackers leveraged compromised infrastructure within Ethereum-based wallets. This was followed by the LIBRA memecoin insider rug pull, which caused $250 million in retail losses and $110 million in insider profits within the Solana ecosystem. The Cetus Protocol attack on the Sui network, exploiting a vulnerability in a third-party math library, drained $223 million through an overflow exploit, marking the largest DeFi incident on Sui to date.

Additional high-profile incidents included Nobitex's $90 million breach (with funds intentionally burned), Phemex's $73 million hot wallet attack, UPCX's $70 million governance vulnerability, and Infini's $49.5 million exploit stemming from overlooked admin privileges. Other notable breaches were linked to smart contract logic flaws (GMX), flash loans (Abracadabra), and oracle manipulation attacks (ResupplyFi and Vicuna).

The leading attack vectors of H1 2025 were access control failures ($1.3B), compromised infrastructure ($1.45B), and logic errors ($350M). These were followed by oracle manipulation and overflow exploits ($230M), private key leaks ($74M), rug pulls ($300M), and social engineering scams ($35M).

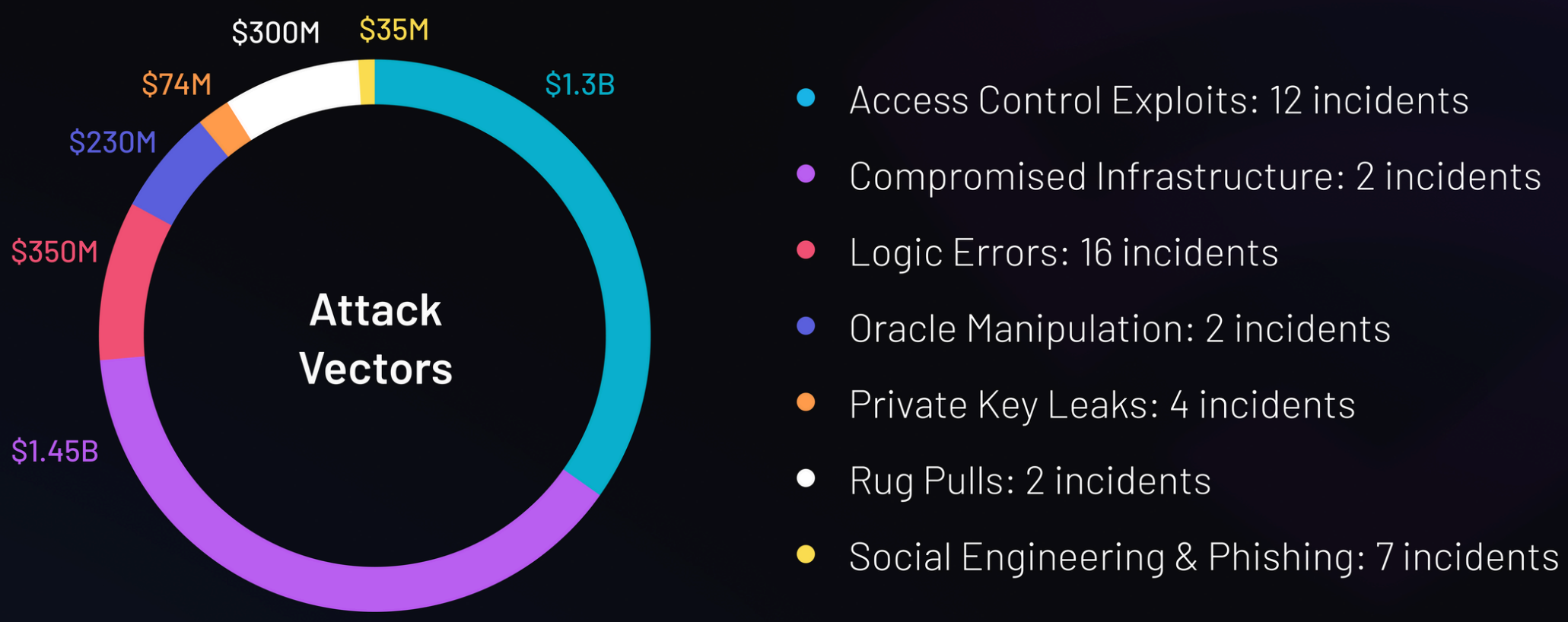
In terms of ecosystem exposure, Ethereum accounted for 65% of total losses, followed by BNB Chain ($250M), Solana ($250M), Sui ($223M), and Arbitrum ($56M). zkSync, Base, and Sonic were also affected, though to a lesser extent. These events reaffirm the growing complexity and cross-chain nature of Web3 threats and underscore the urgent need for robust access controls, secure infrastructure, and proactive smart contract audits.

Current State of Web3 Security – H1 2025

The early months of 2025 were marked by a sharp escalation in Web3 exploits; spike between February and May was largely fueled by landmark incidents such as the $1.45B Bybit compromise, the LIBRA insider rug pull, and the $223M Cetus Protocol exploit on the Sui network.

Access control failures ($1.3B), compromised infrastructure ($1.45B), and logic flaws ($350M) dominated the threat landscape. Other attack vectors included oracle manipulation, overflow bugs, rug pulls, and social engineering exploits—together underscoring the diverse and evolving nature of vulnerabilities in the ecosystem.

On the chain level, Ethereum bore the brunt with ~65% of total losses, followed by BNB Chain and Solana, each accounting for ~$250M. Other impacted ecosystems included Sui, Arbitrum, zkSync, Base, and Sonic, revealing the increasing cross-chain surface area exploited by attackers.



Chain-Wise Impact

Top 10 Hacks 2025 by Amount Lost

The first half of 2025 saw multiple high-impact breaches across exchanges and DeFi protocols, collectively contributing to the majority of losses in the Web3 ecosystem. Below are the ten most significant incidents:

Bybit ETH

$1.45 billion

Compromised Infrastructure

On February 21, 2025, Bybit became the victim of the largest DeFi exploit to date, losing approximately 400,000 ETH (worth ~$1.45 billion). Attackers compromised a developer's machine and inserted malicious JavaScript into the Safe{Wallet} UI. This tampered with transaction parameters invisibly, leading three multisig signers to unknowingly approve a contract upgrade that allowed a full vault drain. Forensic analysis later linked the attack to the Lazarus Group, a North Korea-affiliated hacking unit.

LIBRA – Insider Rug Pull SOL

$250M Retail Losses, $110M Insider Gains

Rug Pull

In mid-February 2025, Argentine President Javier Milei promoted a Solana-based memecoin called $LIBRA—allegedly intended to "fund Argentina's development"—which leapt to a $4.4–4.6 billion FDV within hours. Investigations later revealed that over 80% of the token supply was pre-allocated to insiders, especially Kelsier Ventures, who profited roughly $110 million from early liquidity withdrawals. Retail investors, however, were reportedly caught off-guard: according to blockchain analytics firm Nansen, over 86% of traders suffered losses, totaling approximately $250 million. The scandal—dubbed "Cryptogate"—triggered over 100 criminal complaints in Argentina and a class-action complaint in New York, while allegations of deceptive promotion circulated. Milei has since faced fraud charges in Argentina amid continuing legal and political fallout.

Cetus Protocol SUI

$223 Million Overflow Exploit

Integer Overflow

On May 22, 2025, the Sui-based DEX Cetus suffered a catastrophic exploit resulting in the loss of approximately $223 million—the largest DeFi hack on the Sui network to date. The attacker exploited a vulnerability in the checked_shlw function of a shared math library used by Cetus, triggering an integer overflow in the liquidity calculation logic. By supplying minimal spoofed tokens within narrow tick ranges, the attacker was allocated excessive LP tokens, which were then redeemed for real assets like SUI and USDC. The protocol's treasury was drained almost entirely in a flash-loan-based attack that lasted only minutes. Sui validators later froze an estimated $160 million in stolen funds. The exploit raised serious concerns about the reliability of third-party libraries and the lack of overflow protections in audited codebases.

OWASP Mapping →

Nobitex

$89–90 Million Burn Hack

Access Control Exploit

On June 18, 2025, Iran's largest crypto exchange, Nobitex, was hacked by the politically motivated group Gonjeshke Darande ("Predatory Sparrow"). The attackers drained nearly $90 million and deliberately burned the stolen funds by sending them to irrecoverable vanity addresses. Anti-regime messages were embedded in the transactions, signaling the group's intention to make a political statement rather than profit from the theft.

Phemex BNB

$70–73 Million Hot Wallet Breach

Private Key Leak

On January 23, 2025, Singapore-based exchange Phemex lost approximately $70–73 million after attackers accessed its hot wallets across 16 blockchains. Although cold storage remained secure, the breach caused an immediate suspension of withdrawals. Subsequent investigation revealed ties to infrastructure previously linked to the Lazarus Group, suggesting the possibility of a state-sponsored operation.

UPCX ETH

$70 Million Token Drain via Contract Upgrade

Access Control Exploit

In early April 2025, payment infrastructure protocol UPCX was exploited through an unauthorized proxy admin upgrade. The attacker drained approximately 18.4 million UPC tokens (worth ~$70 million) from three management wallets. Cyvers Security flagged the suspicious transaction, and UPCX suspended deposits and withdrawals shortly thereafter. The incident highlighted poor contract governance and the lack of multi-party authorization in critical admin controls.

0xInfini ETH

$49.5 Million via Privileged Backdoor

Access Control Exploit

On February 24, 2025, a rogue developer exploited lingering admin privileges in Infini's Morpho MEVCapital vault to drain approximately $49.5 million USDC. The attacker executed two large withdrawals, converted the funds to DAI and then to 17,696 ETH, which were later laundered through Tornado Cash. The exploit stemmed from failure to revoke the special "0x8e0b" withdrawer role—a critical access control oversight.

Abracadabra (SPELL) ARB

$13 Million Flash Loan Liquidation Exploit

Logic Error Exploit

On March 25, 2025, lending protocol Abracadabra was exploited for approximately 6,260 ETH (~$13 million) through a flash loan attack targeting its GMX-backed cauldron contracts. The attacker manipulated the borrowing and liquidation mechanics by creating an artificial position that allowed them to borrow assets and immediately liquidate themselves within the same transaction. This bypassed normal collateral requirements and allowed the attacker to extract funds while keeping liquidation incentives. While GMX's core systems were unaffected, the incident highlighted flawed integration logic in Abracadabra's vaults.

OWASP Mapping →

Ionic Protocol MODE

$12.3 Million Fake Token Attack

Social Engineering

On February 4, 2025, the Ionic Protocol on Mode Network was attacked through social engineering. The attacker created a fake LBTC token and convinced the Ionic team to list it, providing a $400K Balancer pool and fake oracle data. They minted LBTC, used it as collateral, borrowed real assets, and bridged them out to Ethereum. A sequencer freeze on Mode managed to recover $8.8 million of the total ~$12.3 million stolen.

ResupplyFi ETH

$9.56 Million via ERC-4626 Oracle Manipulation

Logic Error Exploit

On June 26, 2025, ResupplyFi was exploited through a vulnerability in its ERC-4626 vault logic. The attacker manipulated the vault's exchangeRate using a carefully constructed initial donation, which caused a divide-by-large-number error that made collateral ratios meaningless. This allowed them to borrow ~$9.56 million in reUSD with negligible collateral and drain the vault within hours of deployment.

OWASP Mapping →

Current Challenges with Web3 Security

The Web3 ecosystem continues to grow at an unprecedented pace, yet security mechanisms have not evolved proportionately. As a result, protocols, exchanges, and users remain vulnerable to sophisticated attacks and systemic weaknesses. The major challenges shaping the current state of Web3 security are:

1. Evolving Attack Vectors

- Continuous emergence of zero-day vulnerabilities that evade existing detection systems.
- Rise of multi-vector attacks blending phishing, social engineering, and smart contract logic flaws.
- Flash loan and oracle manipulation exploits bypass traditional defenses, enabling rapid and large-scale fund drains.

2. Inadequate Security Audits

- Many protocols still undergo surface-level or rushed audits before deployment.
- Manual-only audits often fail to identify complex vulnerabilities such as reentrancy, access control flaws, and unsafe external integrations.
- Lack of continuous post-deployment security monitoring, leaving deployed protocols exposed over time.

3. Rapid DeFi Innovation vs. Security Maturity

- Rapid, competitive development cycles lead to untested, unverified, and composable codebases.
- Cross-chain bridges and Layer 2 solutions create new and unaddressed attack surfaces.
- Interoperable protocols increase the blast radius of exploits, allowing one breach to cascade through multiple ecosystems.

4. Centralization Risks

- Centralized exchanges (CEXs) remain the largest targets, accounting for ~65% of H1 2025 losses.
- Compromised private keys, hot wallets, and admin access have led to catastrophic single-point-of-failure breaches.
- Insider threats are still under-addressed, with limited mechanisms for internal access control and monitoring.

5. Lack of Security Standards & Regulations

- Absence of globally recognized smart contract security benchmarks hinders consistent practices.
- Fragmented compliance requirements across jurisdictions lead to inconsistent enforcement.
- Limited adoption of established frameworks like OWASP Smart Contract Security Top 10, delaying industry-wide standardization.

6. Underutilization of AI & Automation

- Manual-heavy security practices dominate, slowing threat detection and increasing operational risk.
- AI-powered tools (e.g., SolidityScan with 450+ automated vulnerability detectors) are underused, despite proven effectiveness.
- The industry remains reactive to breaches rather than leveraging proactive, AI-driven threat intelligence and remediation.

7. Limitations of Existing Automated Tools

- Current automated scanners offer limited vulnerability coverage, generate false positives, and have long scan times.
- Lack of seamless integration with developer workflows and CI/CD pipelines hinders adoption.
- Insufficient real-time monitoring and automated patching, leaving protocols exposed between scans and manual fixes.

8. Fragmentation and Lack of Data Sharing

- The Web3 security landscape is fragmented, with few unified threat intelligence platforms.
- Past hacks and attack patterns are not systematically documented or shared, slowing collective learning.
- This lack of collaboration delays the development of strong, ecosystem-wide defenses.

Way Forward in Web3 Security

1. Proactive Security-First Development

- Integrate security checks throughout the development lifecycle.
- Adopt secure-by-design principles, including robust access controls and transaction validation.
- Enforce real-time vulnerability detection with continuous scanning.

2. Advanced AI-Powered Threat Detection

- Leverage AI-driven scanners (like SolidityScan) to detect complex vulnerabilities.
- Use machine learning models to predict attack patterns and generate automated patches.
- Deploy AI-based threat intelligence systems to mitigate zero-day exploits.

3. Comprehensive Audit Ecosystem

- Combine manual reviews and automated tools for holistic coverage.
- Implement continuous post-deployment monitoring and incident response protocols.
- Utilize bug bounty programs for ongoing security validation.

4. Cross-Chain & Bridge Security Enhancements

- Develop security frameworks tailored for bridges and interoperability solutions.
- Introduce transaction throttling and circuit breakers to mitigate cascading failures.
- Strengthen oracle data integrity to prevent manipulation attacks.

5. Decentralized Infrastructure Hardening

- Implement multi-sig wallets and hardware-based key management.
- Minimize central points of failure using decentralized governance structures.
- Regularly audit infrastructure for compromised admin access and insider threats.

6. Global Security Standards with OWASP Alignment

- Advocate for globally recognized benchmarks like the OWASP Smart Contract Security Top 10 as the foundation for secure dApp development.
- Highlight CredShields' contribution to drafting OWASP smart contract standards, reinforcing thought leadership.
- Encourage protocols to align their audits and testing practices with OWASP guidelines to achieve baseline security assurance.

7. Security Education and Talent Development

- Launch specialized training programs to grow Web3 cybersecurity talent.
- Organize developer workshops on secure smart contract practices aligned with OWASP standards.
- Build open-source educational repositories for community-wide access.

8. Ecosystem-Wide Collaboration

- Promote threat intelligence sharing among auditors, chains, and dApps.
- Foster alliances for collective defense against emerging exploits.
- Host hackathons and security summits to drive security innovation.

Partners & Resources

Our mission to secure Web3 is powered by strong partnerships and a growing knowledge ecosystem. With 490+ vulnerability detectors, AI-driven remediation, and compliance mapping to OWASP Smart Contract Top 10, we've partnered with leading explorers, security platforms, and blockchain ecosystems worldwide.

PARTNERS

Etherscan · Blockscout · REMIX · Rootstock · Etherlink

Immunefi · Dôjima · HackenProof · Soneium · arthera

AVALANCHE · AVASCAN · XDC NETWORK · OPTIMISM · RESONANCE

Linea · SOLIDProof · Reef · hemi · SUBSCAN

JAPAN OPEN CHAIN · BuildBear · Camino · 5ire · BASE

Visual Studio Code · Asset Chain · ASTAR · BLOCKCHAIR · CYBERCENTRY

GATEWAY TO WEB3 SECURITY INSIGHTS

- CredShields ↗
- SolidityScan ↗
- Web3 HackHub ↗
- Security Blogs ↗
- Discover Web3 Security ↗
- OWASP Smart Contract Security Top 10 ↗

CRED SHIELDS

CREDSHIELDS TECHNOLOGIES PTE. LTD.

20A Tanjong Pagar Road, Singapore - 088443