# 46% of crypto lost from exploits is due to traditional Web2 flaws – Immunefi

A new report from blockchain security platform Immunefi suggests that nearly half of all crypto lost from Web3 exploits is due to Web2 security issues such as leaked private keys. The report, released on Nov. 15, looked back at the history of crypto exploits in 2022, categorizing them into different types of vulnerabilities. It concluded that a full 46.48% of the crypto lost from exploits in 2022 was not from smart contract flaws but rather from "infrastructure weaknesses" or issues with the developing firm's computer systems.

Categories of Web3 vulnerabilities. Source: Immunefi

When considering the number of incidents instead of the value of crypto lost, Web2 vulnerabilities were a smaller portion of the total at 26.56%, although they were still the second-largest category.

Immunefi's report excluded exit scams or other frauds, as well as exploits that occurred solely because of market manipulations. It only considered attacks that occurred because of a security vulnerability. Of these, it found that attacks fall into three broad categories. First, some attacks occur because the smart contract contains a design flaw. Immunefi cited the BNB Chain bridge hack as an example of this type of vulnerability. Second, some attacks occur because, even though the smart contract is designed well, the code implementing the design is flawed. Immunefi cited the Qbit

hack as an example of this category.

Finally, a third category of vulnerability is “infrastructure weaknesses,” which Immunefi defined as “the IT-infrastructure on which a smart contract operates—for example virtual machines, private keys, etc.” As an example of this type of vulnerability, Immunefi listed the Ronin bridge hack, which was caused by an attacker gaining control of five out of nine Ronin nodes validator signatures.

Related: Uniswap DAO debate shows devs still struggle to secure cross-chain bridges

Immunefi broke down these categories further into subcategories. When it comes to infrastructure weaknesses, these can be caused by an employee leaking a private key (for example, by transmitting it across an insecure channel), using a weak passphrase for a key vault, problems with tw-factor authentication, DNS hijacking, BGP hijacking, a hot wallet compromise, or using weak encryption methods and storing them in plaintext.

While these infrastructure vulnerabilities caused the greatest amount of losses compared to other categories, the second-largest cause of losses was “cryptographic issues” such as Merkle tree errors, signature replayability and predictable random number generation. Cryptographic issues resulted in 20.58% of the total value of losses in 2022.

Another common vulnerability was “weak/missing access control and/or input validation,” the report stated. This type of flaw resulted in only 4.62% of the losses in terms of value, but it was the largest contributor in terms of the number of incidents, as 30.47% of all incidents were caused by it.

Source link