Port3 Network
@Port3Network

Incident Report: $PORT3 Hacker Attack

PORT3 aimed to support the development of multiple chains, and therefore adopted @nexa_network's cross-chain token solution, CATERC20. However, CATERC20 contained a boundary-condition validation vulnerability. After the token's ownership was renounced, the function returned a value of 0, which happened to match the owner-verification condition.

As a result, the ownership check failed and unauthorized access became possible. This issue was not identified in the CATERC20 audit report. Since the Port3 Token had previously renounced ownership for greater decentralization, it was in exactly this vulnerable state.

🧶 (1/3)

5:51 AM · Nov 23, 2025 · **74.9K** Views

Port3 Network
@Port3Network

(2/3)
The hacker discovered this authorization-verification bug in the PORT3 contract.
At 20:56:24 PM UTC, using address 0xb13A503dA5f368E48577c87b5d5AeC73d08f812E, the hacker initiated a RegisterChains operation, registering his own address as an address authorized to perform BridgeIn operations.

At the same time, the hacker deployed a fake token on the Arbitrum One chain and initiated a cross-chain transaction. Due to the flaw in the BSC-side Port3 token contract, the validation incorrectly passed, resulting in the minting of 1 billion tokens. The hacker then sold these tokens on DEXs, causing a rapid price crash.

5:51 AM · Nov 23, 2025 · **30.3K** Views

Port3 Network
@Port3Network

(3/3)
The attacker subsequently repeated the same exploit from other addresses, including:
0x7C2F4Bbda350D4423fBa6187dc49d84D125551fF

We have contacted major exchanges to suspend deposits and withdrawals.
Moving forward, we will fix the issue by reissuing the token with a new contract.

5:52 AM · Nov 23, 2025 · **26.2K** Views