What is a delegatecall bug?

`delegatecall` is a low-level Solidity operation that executes another contract's code in the calling contract's own storage, balance, and `msg.sender` context. It powers upgradeable proxies, but it is dangerous: if the target is attacker-controlled, or the called code modifies storage slots that mean something different in the caller, an attacker can overwrite critical state (like the owner) or take over the contract. The fix is to delegatecall only trusted, immutable targets and align storage layouts. It maps to SWC-112.

HOW IT WORKS

01 How it works and example

Two classic failures:

- Untrusted target: a contract delegatecalls to an address the attacker controls (for example, set via an unprotected function). The attacker's code runs in the contract's context and overwrites the owner slot, then drains it. The Parity multisig incidents stemmed from delegatecall/-`selfdestruct` on shared library code.
- Storage collision: the implementation's variable layout does not match the proxy's, so writing one variable corrupts another (for example the admin slot). See proxy storage collision.

Documented for defensive context.

> THEIR CODE, YOUR STORAGE
>
> `delegatecall` *runs someone else's code against your storage and as your identity. Only ever delegatecall to trusted, fixed code, and make sure storage layouts line up exactly.*

HOW TO DEFEND

- Only delegatecall trusted, immutable targets, never an address an attacker can set or influence.
- Use battle-tested proxy patterns (standard upgradeable proxy libraries) rather than hand-rolling delegatecall.
- Align storage layouts between proxy and implementation (use unstructured/EIP-1967 storage slots) to avoid collisions.
- Protect upgrade and target-setting functions with strong access control.
- Audit every delegatecall path and the proxy/implementation pairing.

SOURCES

[1] SWC Registry: Smart Contract Weakness Classification

[2] Solidity docs: Security considerations

[3] MITRE CWE-829: Inclusion of Functionality from Untrusted Control Sphere