

Reentrancy Attack

[Return to Glossary](#)

Reentrancy Attack occurs when the attacker drains funds from the target by recursively calling the target's withdraw function. When the contract fails to update its state, a victim's balance, prior to sending funds, the attacker can continuously call the **withdraw** function to drain the contract's funds. A famous real-world Reentrancy attack is the Decentralized Autonomous Organization (DAO) attack, which caused a loss of 60 million US dollars.

Source: <https://arxiv.org/pdf/2105.02881.pdf>

From:
<https://www.omgwiki.org/dido/> - **DIDO Wiki**

Permanent link:
https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a_glossary:r:reentrancy_attack&rev=1643905579

Last update: **2022/02/03 11:26**

