bitshares HacktheDex

Report 20180801A

Type

Cross-site scripting (XSS) code injection

Description

The memo of a transfer is user input and allowed HTML. It was insecurely rendered after unlocking the wallet, which allowed execution of arbitrary JavaScript code.

Review

OWASP Rating	
Likelihood	High
Impact	Medium
Severity	High

Possible attack vector: Recognize password input / unlocking of the local wallet and broadcast malicious transactions or collect private keys.

Reviewers: Fabian Schuh, Ryan Fox, Sigve Kvalsvik

Resolution

Alerted HackTheDex subscribers on 16th August of 2018. Fixed by sanitizing user input.

Reward Consensus

Reward	8,000 bitUSD

Reported 2018-08-01 Accepted 2018-08-08 Fixed 2018-08-08