**Problem**

<https://github.com/stellar/js-stellar-sdk/security/advisories/GHSA-6cgh-hjpw-q3gq>

The Utils.readChallengeTx function used in [SEP-10 Stellar Web Authentication](https://github.com/stellar/stellar-protocol/blob/master/ecosystem/sep-0010.md) states in its function documentation that it reads and validates the challenge transaction including verifying that the serverAccountID has signed the transaction. The function does not verify that the server has signed the transaction and has been fixed so that it does in v8.2.3.

Applications that also used Utils.verifyChallengeTxThreshold or Utils.verifyChallengeTxSigners to verify the signatures including the server signature on the challenge transaction are unaffected as those functions verify the server signed the transaction.

Applications calling Utils.readChallengeTx should update to v8.2.3 to ensure that the challenge transaction is completely valid and signed by the server creating the challenge transaction.

<https://github.com/stellar/stellar-protocol/blob/master/ecosystem/sep-0010.md>

**utils.ts**

export function readChallengeTx(

challengeTx: string,

serverAccountID: string,

networkPassphrase: string,

homeDomains: string | string[],

webAuthDomain: string,

): { tx: Transaction; clientAccountID: string; matchedHomeDomain: string } {

…

…

**\*\*** **La fonction ne vérifie pas que le serveur a signé la transaction\*\***

}

**Fix**

**utils.ts**

export function readChallengeTx(

challengeTx: string,

serverAccountID: string,

networkPassphrase: string,

homeDomains: string | string[],

webAuthDomain: string,

): { tx: Transaction; clientAccountID: string; matchedHomeDomain: string } {

…

…

**if (!verifyTxSignedBy(transaction, serverAccountID)) {**

**throw new InvalidSep10ChallengeError(**

**`Transaction not signed by server: '${serverAccountID}'`,**

**);**

**}**

}