Anon Shop

Affected Components

github.com/DecentralizeJustice/anonymousLocker/netlify/functions/loginToAccount.js

github.com/DecentralizeJustice/anonBackend/netlify/functions/proccessSettledBTCpayInvoice.js

CVE-2024-36589

anonshop.app - Password security

An issue was discovered in Annonshop.app's anonymousLocker commit 2b2b4 to ba9fd and anonBackend commit 57837 to cd815, where credentials were found to be stored in plaintext.

Vulnerability Categorisation

Vendor: Anonymous Locker LLC (d/b/a Anonshop)

Product: Anonshop Backend

Vulnerability Type: Password security

Attack Type: Local

Impact: Information disclosure

Attack Vectors: Cleartext Storage of Sensitive Information

Affected Component: loginToAccount.js & proccessSettledBTCpayInvoice.js

Zero-Day Exploitation

Exploited In Wild: Unknown

Notes: There have been no public accounts regarding exploitation occurring.

Vulnerability Attack Vector

To attack this vulnerability one must have access to the database, from there plaintext passwords can be extracted.