

main

...

poc / NCH / ReflectCRM_3.01_CC.md

 0xfml added Reflect Cleartext Creds

History

1 contributor

28 lines (18 sloc) | 662 Bytes

Description

Reflect CRM and earlier stores all user information in configuration files on the local disk. This allows local users to discover cleartext user passwords by reading said files.

Vulnerability type

Cleartext Credential Storage

Vendor

NCH Software

Affected versions

Reflect CRM 3.01 and earlier

Attack type

Local

Authenticated

Yes

Attack vectors

Reflect CRM stores all registered user information in a config file on the local disk. The files contain cleartext username, password and auth level.

User files in: C:\ProgramData\NCH Software\Reflect\WebAccounts\

Link

<https://www.nchsoftware.com/crm/index.html>