Tejas Pingulkar

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

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

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

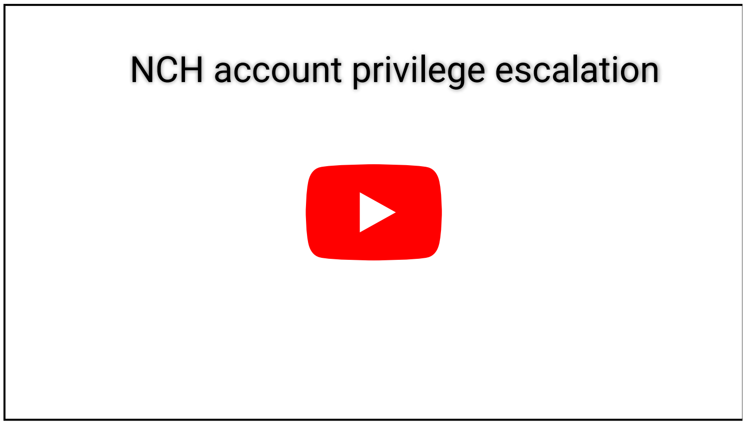
Receipts and Deposits: http://[website:port]/cashtxn?payment=0

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



To leave a comment, click the button below to sign in with Google.

Popular posts from this blog

CVE-2020-23446 Verint Workforce Optimization (WFO)

September 17, 2020

Vulnerable Software : Verint Workforce Optimization (WFO) Vulnerability : Unauthenticated Information Disclosure via API Affected Version: 15.1 (15.1.0.37634) Vendor Homepage: Link CVE: 2020-23446 CVE Author: Tejas Nitin Pingulkar Exploit Available: POC Available About Aff …

READ MORE

NCH Express CVE-2020-11560 Clear Text Password Storage

March 29, 2020

CVE: CVE-2020-11560 Title: Clear text password storage in NCH express invoice software About NCH express invoice software: Express Invoice lets you create invoices you can print, email or fax directly to clients for faster payment. The reporting functionality allows you to keep track of payment …

READ MORE

Follow me on Linked in https://www.linkedin.com/in/tejaspingulkar/

TEJAS PINGULKAR

VISIT PROFILE

Search This Blog

Search this blog

Archive

Labels

Report Abuse

Followers

Followers (1)