NCH Express CVE 2020-11561 Privilege Escalation

March 30, 2020

CVE: CVE-2020-11561
Title: Privilege Escalation via Forceful Browsing

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 payments, overdue accounts, sales team performance and more.

Vulnerability: NCH express invoice 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 "Add New Item" "Add New Customer".
User with viewer privileges don't have access to "Add New Item" "Add New Customer"
by forceful browsing, we will access admin modules using viewer user privileges

Impact: An authenticated low privileged user can access modules which are accessible only to higher privileged user

POC:

CVE   Cyber Security   Exploit

----

saivenkat *July 27, 2020 at 10:15 PM*

My rather long internet look up has at the end of the day been compensated with pleasant insight to talk about with my family and friends.
Best CRM System

REPLY

panindia *February 18, 2021 at 9:10 PM*

ngo foundation in india
Plan india is a child rights organisation providing children, especially girls, with access to education, healthcare, protection and livelihood opportunities. • Plan India is a child rights organization providing children, especially girls, with access to education, healthcare, protection and livelihood opportunities

REPLY

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 Affected Software: Verint …

READ MORE

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: Y es About Affected Software Express Accounts is professio …

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 payments, ov …

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 ⌄

Followers
Followers (1)