CVE-2020-13480-Verint-HTML Injection

June 08, 2020

Vulnerable Software: Verint Workforce Optimization (WFO)

Vulnerability: HTML Injection

Affected Version: 15.2

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

CVE: CVE-2020-13480

CVE Author: Tejas Nitin Pingulkar

Exploit Available: POC Available

About Affected Software

Verint Workforce Optimization is a suite of unified software and services for capturing interactions and managing the performance of employees across the enterprise or in targeted areas of your business, including:

- Back-office operations
- Branch operations
- Contact centers
- Financial trading rooms

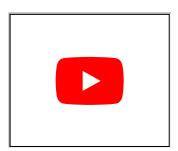
Additional Information

Verint WFO application provides functionality to send receive emails within an application. However application fails to sanitize user input.

Exploit:

- 1. Open send email function
- 2. Write your payload inside the body

POC:



Timeline:

Initial Email Sent: 21 May 2020 — No response Followup 2: 25 May 2020 — No response Followup 3: 26 May 2020 — No response CVE Generated: 26 May 2020 Followup 4:08 June 2020 — No response Published: 09 June 2020



CVEWALKTHROUGH.COM

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

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 i ...

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

B Powered by Blogger

Theme images by Michael Elkan

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

