

## 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 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 download topology reports to authenticated users, however, using direct object reference/API unauthenticated attacker can obtain reports.

### Exploit:

Access URL: [IP/Domain]/wfo/rest/em-api/v1/topology/generation

Note: only most recently generated report can be obtained by the attacker

**Patch:** Patched in version 15.2

### POC:



### Timeline:

- 2 May 2019 – Informed about vulnerability to Telligent.
- 3 May 2019 – Initial response.
- 3 May 2019 – Vulnerability reported.
- 3 May 2019 – Telligent forwarded details to WFO team.
- 7 May 2019 – followup with WFO
- 9 May 2019 – Telligent team confirmed that they will update soon
- 21 May 2019 – followup with WFO
- 21 May 2019 – followup with Telligent Team
- 21 May 2019 – email acknowledgment from Verint (WFO Team)
- 29 May 2019 – followup with WFO

29 May 2019 – followup with Telligent Team

29 May 2019 – Telligent Team replied back

30 May to till date – No response from both Team vulnerability was patched in 15.2 but no acknowledgment

17 September 2019- Vulnerability Published



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



Popular posts from this blog

### 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](#)

Powered by Blogger

Theme images by [Michael Elkan](#)

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)

