

Verint: Unauthenticated Information Disclosure via API

[Home](#) › [Uncategorized](#) › [Verint: Unauthenticated Information Disclosure via API](#)

1 Comment [Uncategorized](#) [tp9222@gmail.com](#) [July 26, 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 attacker

Patch: Patched in version 15.2

POC:

Recent Posts

Protected: Smart Office Suite- Unauthenticated Data Ex

CVE-2021-41716 Mahavitaran Android
Application: Account take over via OTP Fixation

CVE-2020-27413 Mahavitaran Android
Application: Clear-text password storage

CVE-2020-27416 Mahavitaran Android
Application: Account take over via OTP bypass

CVE-2020-35398: UTI Mutual fund Android
Application- Username Enumeration

Archives

December 2022

December 2021

September 2021

August 2021

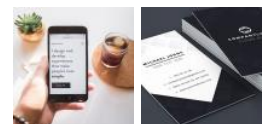
December 2020

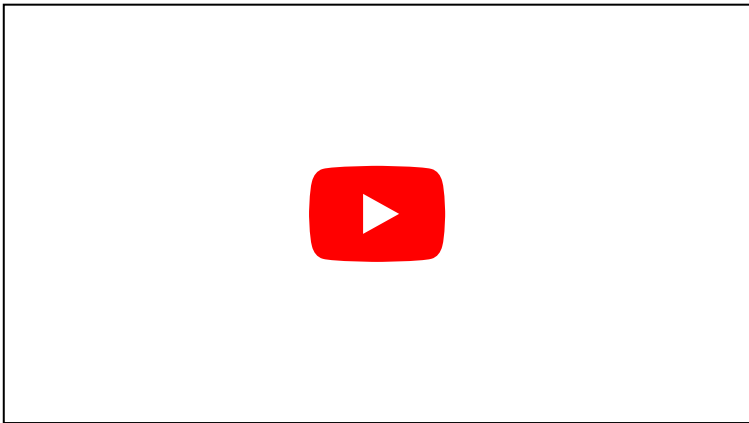
July 2020

June 2020

April 2020

Gallery





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

◀ CVE-2020-13480:Verint Workforce Optimization : HTML Injection CVE-2020-13473: NCH Account-Clear Text Password Storage ▶

One thought on “Verint: Unauthenticated Information Disclosure via API”

Pingback: [CVE.report](#)

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website

☐ Save my name, email, and website in this browser for the next time I comment.

[Post Comment](#)

Copyright © 2020 Mr. Tejas Nitin Pingulkar. Develope by: GSunite Group.

tp9222@gmail.com +91 8149756079