alert3 / **main.txt**

Created 2 years ago

Solarwinds Orion - Web Console WPM: 2019.4.1 Orion Platform HF4, NPM HF2: 2019.4

main.txt

```
1  This is a description of two Stored XSS vulnerability found in Solarwinds Orion - Web Console WPM: 2019.4.1 Orion Platform HF4, NPM HF2: 20
```

alert3 commented on Jun 24, 2020 • edited Author

Product

Solarwinds Orion - Web Console WPM: 2019.4.1 Orion Platform HF4, NPM HF2: 2019.4

Author

Amin Rawah

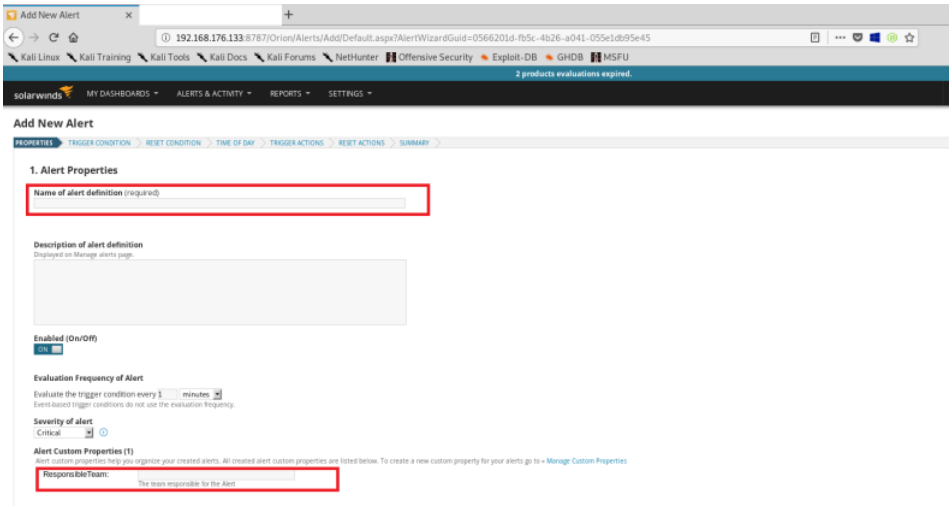
CVE ID

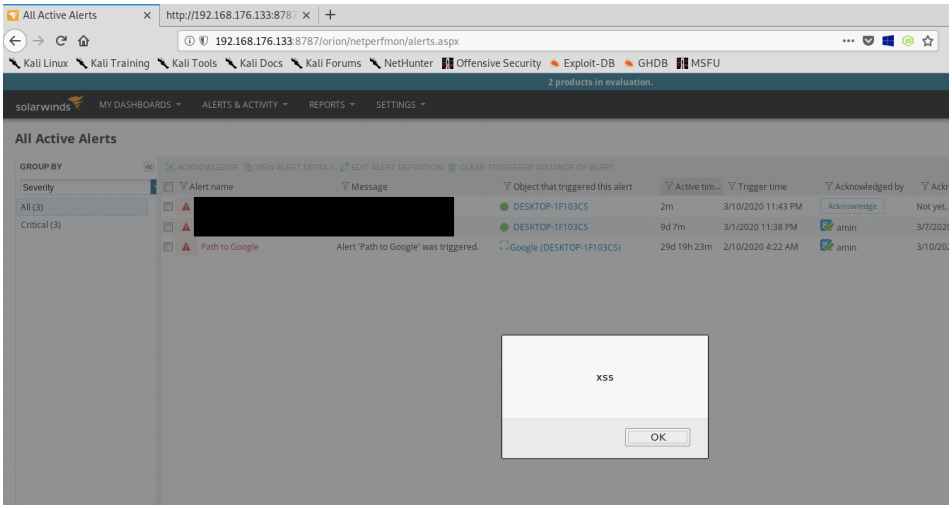
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14006
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14007

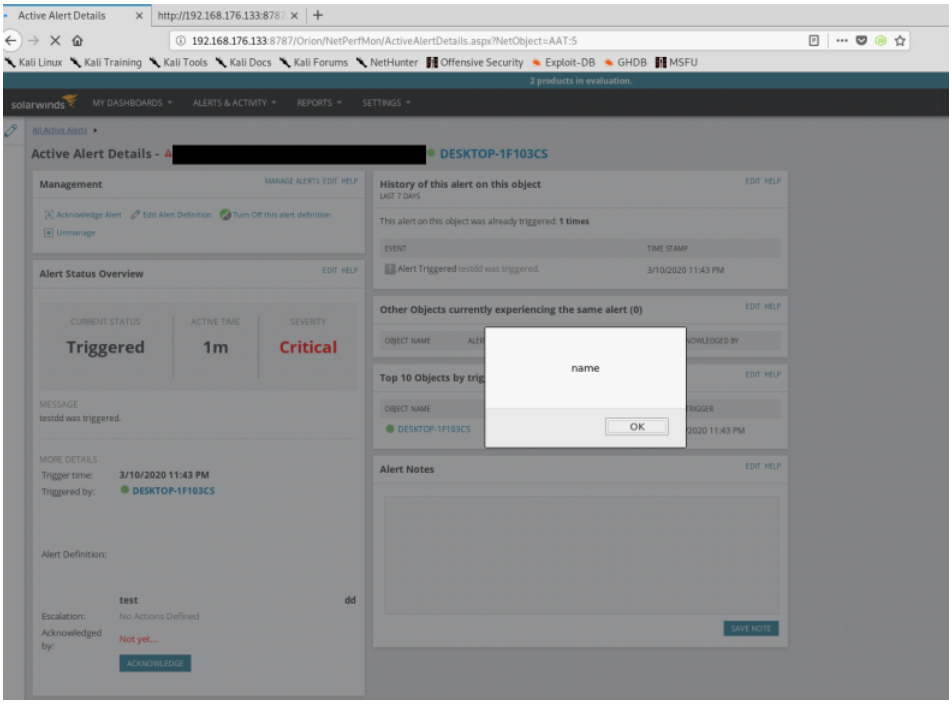
Description

A malicious user with privilege to create **"Alerts"** can create an alert and inject XSS payload in it. There are two injection points one point is more critical since it affects two pages.
While creating a new alert, an attacker can inject in **'name of alert definition'** `<svg/onload=alert('name') />` and **'Responsible Team'** `<svg/onload=alert('XSS') />` to cause stored XSS affecting all users including Admins visiting **"Alerts"** page. The payload injected in **'Responsible Team'** will be executed as soon as a user visit **"Alerts"** page or clicking alert's details, However, the injection in **'name of alert definition'** will be executed when a user click on alert details.

PoC


Add New Alert
192.168.176.133:8787/Orion/Alerts/Add/Default.aspx?AlertWizardGuid=0566201d-fb5c-4b26-a041-055e1db95e45
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
2 products evaluations expired.
solarwinds MY DASHBOARDS ALERTS & ACTIVITY REPORTS SETTINGS
Add New Alert
PROPERTIES TRIGGER CONDITION RESET CONDITION TIME OF DAY TRIGGER ACTIONS RESET ACTIONS SUMMARY
1. Alert Properties
Name of alert definition (required)
Description of alert definition
Displayed on Manage alerts page.
Enabled (On/Off)
ON
Evaluation Frequency of Alert
Evaluate the trigger condition every 1 minutes
Event-based trigger conditions do not use the evaluation frequency.
Severity of alert
Critical
Alert Custom Properties (1)
ResponsibleTeam:
The team responsible for the Alert


All Active Alerts
http://192.168.176.133:8787
192.168.176.133:8787/orion/netperfmon/alerts.aspx
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
2 products in evaluation.
solarwinds MY DASHBOARDS ALERTS & ACTIVITY REPORTS SETTINGS
All Active Alerts
GROUP BY
Severity
All (3)
Critical (3)
Alert name
Message
Object that triggered this alert
Active tim...
Trigger time
Acknowledged by
DESKTOP-1F103CS
2m
3/10/2020 11:43 PM
Acknowledge
DESKTOP-1F103CS
9d 7m
3/1/2020 11:38 PM
amin
Path to Google
Alert 'Path to Google' was triggered.
Google (DESKTOP-1F103CS)
29d 19h 23m
2/10/2020 4:22 AM
amin
xss
OK


Active Alert Details
http://192.168.176.133:8787
192.168.176.133:8787/Orion/NetPerfMon/ActiveAlertDetails.aspx?NetObject=AAT:5
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
2 products in evaluation.
solarwinds MY DASHBOARDS ALERTS & ACTIVITY REPORTS SETTINGS
All Active Alerts
Active Alert Details -
DESKTOP-1F103CS
Management
Acknowledge Alert
Edit Alert Definition
Turn Off this alert definition
Unmanage
History of this alert on this object
LAST 7 DAYS
This alert on this object was already triggered: 1 times
EVENT
TIME STAMP
Alert Triggered testdd was triggered.
3/10/2020 11:43 PM
Alert Status Overview
CURRENT STATUS
ACTIVE TIME
SEVERITY
Triggered
1m
Critical
Other Objects currently experiencing the same alert (0)
OBJECT NAME
Top 10 Objects by trig
OBJECT NAME
DESKTOP-1F103CS
name
OK
MESSAGE
testdd was triggered.
MORE DETAILS
Trigger time:
3/10/2020 11:43 PM
Triggered by:
DESKTOP-1F103CS
Alert Definition:
test
dd
Escalation:
No Actions Defined
Acknowledged by:
Not yet...
ACKNOWLEDGE
Alert Notes
SAVE NOTE