

Instantly share code, notes, and snippets.

alert3 / main.txt

Created 2 years ago

☆ Star

<> Code ↻ Revisions 1

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: 2019.4

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.

**Add New Alert**

1. Alert Properties

Name of alert definition (required)

Description of alert definition

Enabled (On/Off)

Evaluation Frequency of Alert

Severity of alert

Alert Custom Properties (1)

ResponsibleTeam: The team responsible for the Alert

**All Active Alerts**

Severity	Alert name	Message	Object that triggered this alert	Active time	Trigger time	Acknowledged by	Acknowledged
All (3)			DESKTOP-1F103CS	2m	3/10/2020 11:43 PM		Not yet
Critical (3)			DESKTOP-1F103CS	9d 7m	3/1/2020 11:38 PM	amin	3/7/2020
	Path to Google	Alert 'Path to Google' was triggered.	Google (DESKTOP-1F103CS)	29d 19h 23m	2/10/2020 4:22 AM	amin	3/10/2020

XSS

OK

**Active Alert Details**

DESKTOP-1F103CS

Management

Alert Status Overview

Current Status: Triggered

Active Time: 1m

Severity: Critical

Message: testdd was triggered.

More Details

Trigger time: 3/10/2020 11:43 PM

Triggered by: DESKTOP-1F103CS

Alert Definition:

test

Escalation: No Actions Defined

Acknowledged by: Not yet...

Alert Notes

name

OK