##
Exploit Title: Open-AudIT Community - 2.2.6 - Cross Site Scripting Vulnerability
Google Dork:NA
##
Exploit Author: Ranjeet Jaiswal#
##
Vendor Homepage: https://opmantek.com/
Software Link:https://opmantek.com/network-tools-download/open-audit/
Affected Version: 2.2.6
Category: WebApps
Tested on: Windows 10
CVE : CVE-2018-14493
#
1. Vendor Description:
#
Network Discovery and Inventory Software | Open-AudIT | Opmantek
Discover what's on your network
Open-AudIT is the world's leading network discovery, inventory and audit program. Used by over 10,000 customers.
#
2. Technical Description:
#
#Cross-site scripting (XSS) vulnerability on Groups Page in Open-AudIT Community edition in 2.2.6 allows remote attackers to inject arbitrary web script or HTML in group name,as demonstrated in below POC.
#
3. Proof Of Concept:

3.1. Proof of Concept for Injecting html contain

#Step to reproduce.
Step1:Login in to Open-Audit
Step2:Go to Group page
Step3:Select any group which are listed
Step4:click on "Details tab".
Step5:In the Name field put the following payload and saveit.

Sorry! We have moved! The new URL is: Open-Audit

Step6:Click on "View Tab" in which payload is put.
Step7:When user Click on View Tab.User will see redirection hyperlink.
Step8:When user click on link ,User will be redirected to Attacker or malicious website.

3.2. Proof of Concept for Injecting web script(Cross-site scripting(XSS))

#Step to reproduce.
Step1:Login in to Open-Audit
Step2:Go to Groups page
Step3:Select any group which are listed
Step4:click on "Details tab" in which payload is put.
Step5:In the Name field put the following payload and Saveit.

<script>alert(hack)</script>

Step6:Click on "View Tab" of group in which payoad is put.
Step7:When user Click on View Tab an Alert Popup will execute.

4. Solution:
#
Upgrade to latest release of Open-AudIT version
  Please visit below link to get news on latest version of Open-AudIT release.
https://community.opmantek.com/display/OA/Release+Notes