Shubham pandey Follow

May 12 · 2 min read · Listen

XSS Found In Nokia G-2425G-A Home WIFI Router

 # Exploit Title: Nokia “G-2425G-A” Bharti Airtel Routers Hardware version “3FE48299DEAA” Software Version “3FE49362IJHK42” is vulnerable to Cross-Site Scripting (XSS) via admin->Maintenance>Device Management.

#Exploit Author: Shubham Pandey

#vendor: Nokia | Airtel

#Application Link: https://www.indiamart.com/proddetail/nokia-ont-g-2425g-a-gpon-ont-router-23710241448.html

#Hardware version “3FE48299DEAA” Software Version “3FE49362IJHK42”

What is Stored XSS :

XSS is Stand for Cross-Site Scripting. Stored XSS is a type of XSS. In Which an attacker permanently injects the malicious javascript into the database of the target server. A common impact of XSS is that the attacker can steal the cookies of users, deface the web application, and redirect the user’s to phishing pages.

Stored XSS is also known as Persistent XSS.

Attack Vector:

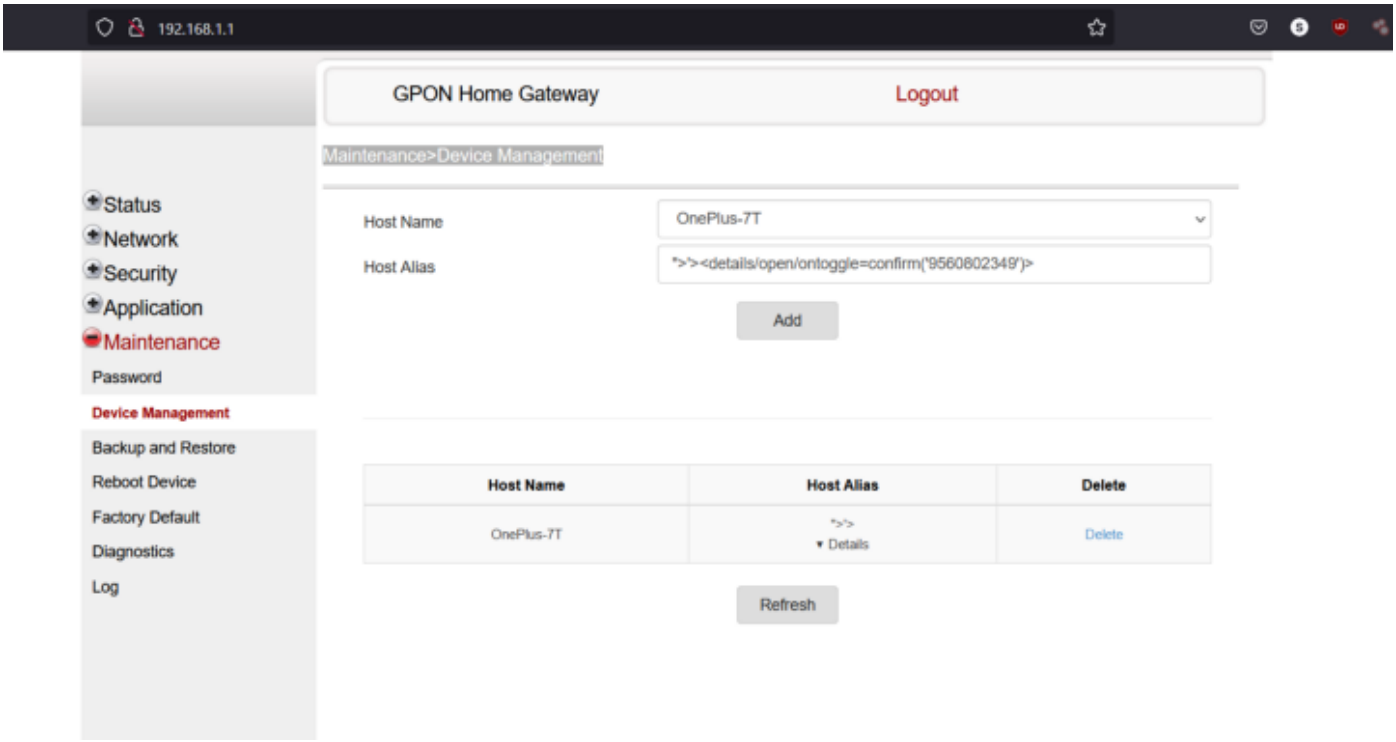
An attacker injects the XSS payload in Device Management in the place where the user can set Host Alias, Now each time user visits the application the XSS triggers, and the Attacker can redirect the user to some malicious or phishing webpages according to the crafted payload.

Vulnerable Parameter: "admin->Maintenance>Device Management."

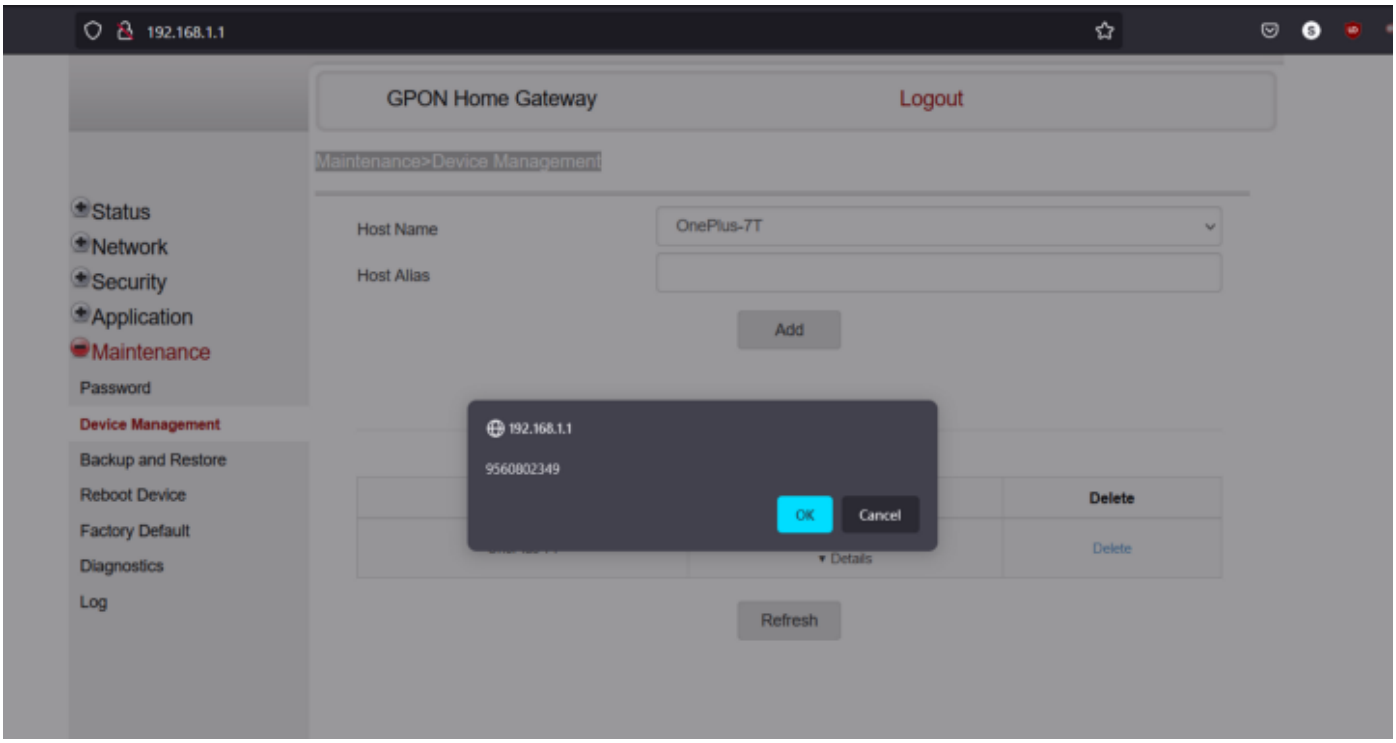
Steps to Reproduce:

1. Go to Maintenance>Device Management
2. Fill in the details and Put a payload on the "Host Alias="

">'><details/open/ontoggle=confirm('9560802349')>



3. Router Application Accept the payload and stored it permanently until someone deletes it intently.



Video POC

Author: Shubham Pandey

https://www.linkedin.com/in/shubham-pandey-10704014b