

Thiago "THX" Sena - FireShell Security Team

Mail:thiagosena@outlook.com

About the Software:

<http://www.tp-link.com.br/products/details/TL-MR3220.html>

[Vulnerability]

- There is XSS in Wireless MAC Filtering, where it is in Wireless; Wireless MAC Filtering

[Type of vulnerability]

- Cross Site Scripting (XSS)

[Product Salesperson]

- <http://www.tp-link.com.br>

[Affected Component]

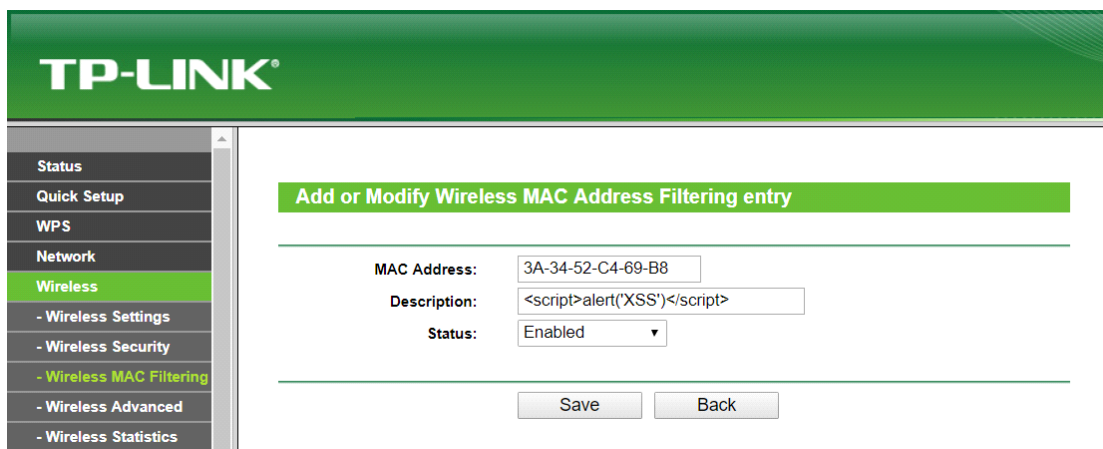
- TP-LINK TL-MR3220

[Type of attack]

Remote

[Attack Vectors]

- In the 'Wireless MAC Filtering' tab, you will add a new MAC Address, in 'Description' it will put the script (`<script>alert('XSS')</script>`) and complete the registration.



The screenshot displays the TP-LINK web interface. At the top, the TP-LINK logo is visible. On the left, a navigation menu lists various settings: Status, Quick Setup, WPS, Network, Wireless (highlighted), - Wireless Settings, - Wireless Security, - Wireless MAC Filtering (highlighted), - Wireless Advanced, and - Wireless Statistics. The main content area is titled 'Add or Modify Wireless MAC Address Filtering entry'. It contains three input fields: 'MAC Address' with the value '3A-34-52-C4-69-B8', 'Description' with the value '<script>alert('XSS')</script>', and 'Status' with a dropdown menu set to 'Enabled'. At the bottom of the form, there are two buttons: 'Save' and 'Back'.

TP-LINK®

00:0E:17:31:70:02
XSS

OK

Status

Quick Setup

WPS

Network

Wireless

- Wireless Settings

- Wireless Security

- Wireless MAC Filtering

- Wireless Advanced

- Wireless Statistics