

CVE-2019-16412

[Description]

In goform/setSysTools on Tenda N301 wireless routers, attackers can trigger a device crash via a zero wanMTU value. (Prohibition of this zero value is only enforced within the GUI.)

[Additional Information]

On Tenda N301 wireless routers "wan MTU=" parameter value validation only client sided. If an attacker in GUI interface sent a valid MTU value, but catch the data (for example use Burp Suite application!) sent and set "&wanMTU=" value zero, and transmitted modified data, this resulted hardware crash. This is because the data received from the client is not validated on the server side.

Tenda N301 wireless router.



Tenda N301 wireless router GUI. Not enabled zero value MTU parameter.

The screenshot shows the Tenda N301 wireless router GUI. The left sidebar contains navigation links: Status, Internet Settings, Wireless Settings, Bandwidth Control, Wireless Repeating, Parental Controls, Advanced, and Administration (highlighted). The main content area is titled 'Login Password' and 'WAN Parameters'. Under 'WAN Parameters', the MTU is set to 0, with a red box around it and a message 'Input range is: 576 - 1500'. The Clone MAC is set to 'Restore Factory MAC' and the WAN Speed is set to 'Auto'. The LAN Parameters section is partially visible at the bottom.

Set zero value.

The screenshot shows the Burp Suite Community Edition v1.7.36 interface. The 'Intercept' tab is active, showing an intercepted HTTP request to http://192.168.0.1:80. The request body is displayed in the 'Raw' tab, showing a POST request to /js/form/setSysTools HTTP/1.1. The request body contains a parameter 'swanMTU=1400' which is highlighted with a red box and labeled 'Set zero value'.

Crashed router!!



[VulnerabilityType Other]

denial of service (total hardware crash!)

[Vendor of Product]

<https://www.tendacn.com/>

[Affected Product Code Base]

Tenda Wireless router - N301

[Affected Component]

POST /goform/setSysTools
"&wanMTU="

[Attack Type]

Remote

[Impact Denial of Service]

true

[Attack Vectors]

POST /goform/setSysTools
POST_DATA:
"&wanMTU=[Set wanMTU value 0]" --> "&wanMTU=0"

[Reference]

<https://www.tendacn.com/>