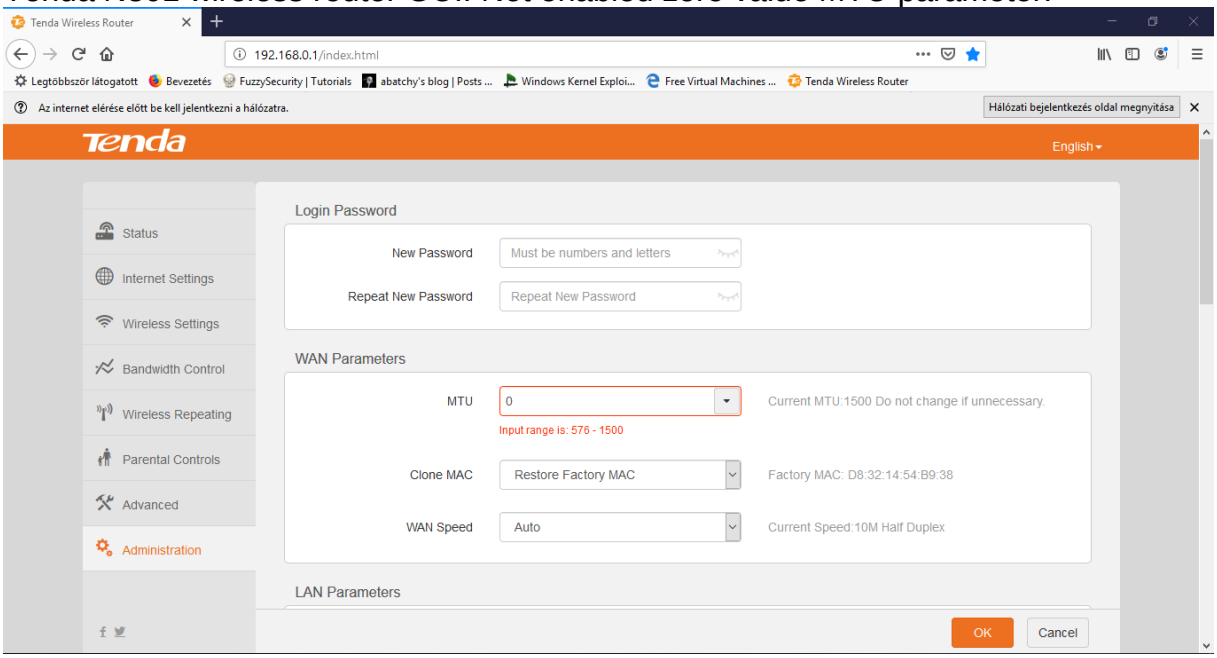
CVE-2019-16412

[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.)

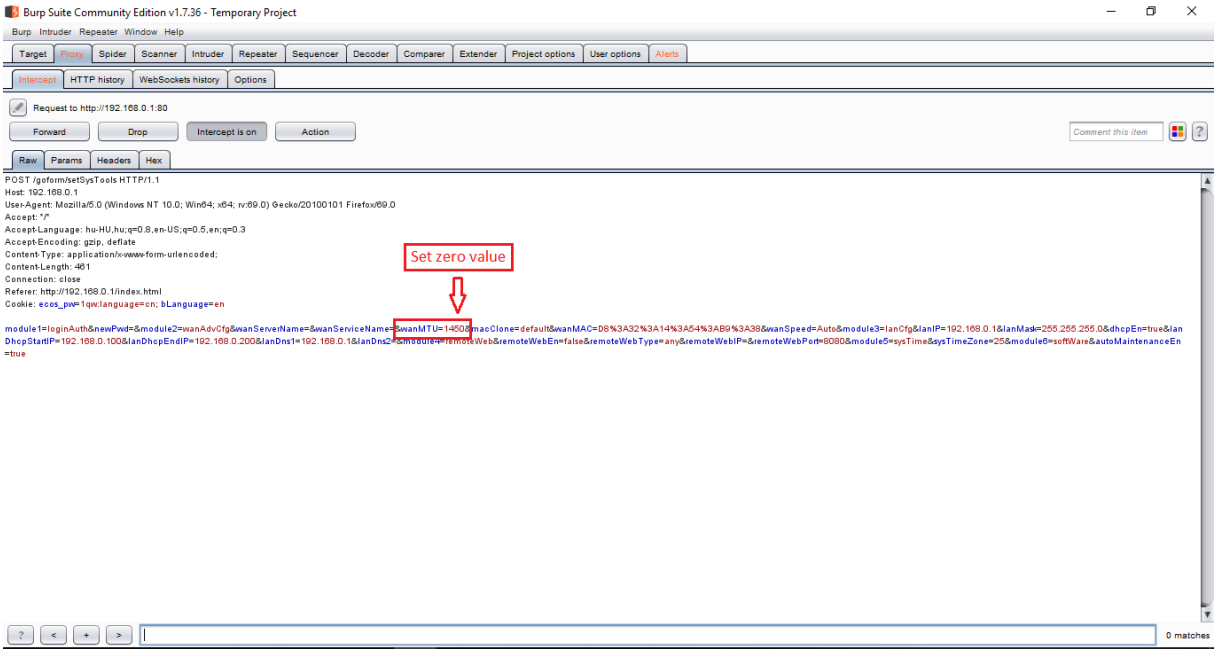
[Additional Information]
On Tenda N301 wireless routers "wan MTU=" parameter value validation only client sided. If an attacker in GUI interface sent a valid MTU value, but catch the data (for example use Burp Suite application!) sent and set "&wanMTU=" value zero, and transmitted modified data, this 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.



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/