Tenda AC18(V15.03.05.19) has a Stack Buffer Overflow Vulnerability

Product

1. product information:
2. firmware download:

Affected version

V15.03.05.19

Vulnerability

The stack overfow vulnerability is in /bin/httpd. The vulnerability occurrs in the `fromSetSysTime` function, which can be accessed through the URL `/goform/SetSysTimeCfg`.

The `v20` variable is directly retrieved from the http request parameter `time`.

Then `v20` will be splice to stack by function `sscanf` without any security check,which causes stack overflow.