Tenda AC15(V15.03.05.18) has a Buffer Overflow Vulnerability

Product

1. product information:
2. firmware download:

Affected version

V15.03.05.18

Vulnerability

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

In function `formSetPPTPServer`, The `sscanf` function is used to copy the sent post data `startip` and `endip` onto the stack, causing a stack overflow.