Netpilot Soho Blue – Privilege Escalation

http://www.sohoblue.com/

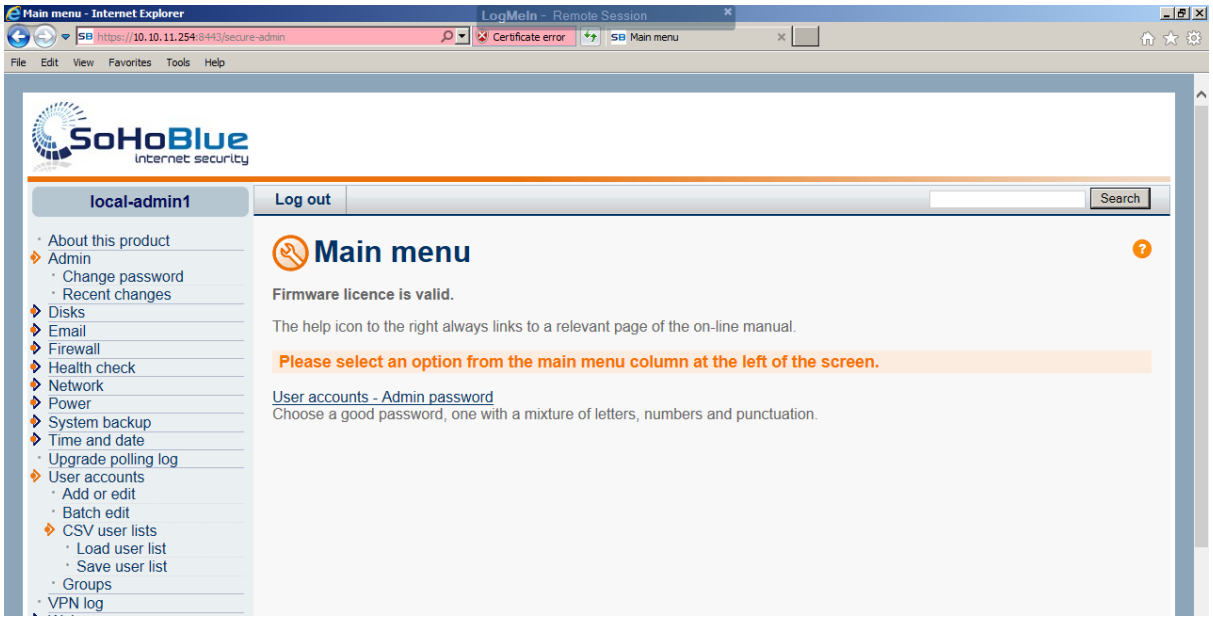
Author Richard Davy
Email – rmdavy@rmdavy.karoo.co.uk
Product SoHo Blue
Software Version 6.1.15 (upgraded)

Privilege Escalation from site-admin to admin and also password decryption.

NetPilot Soho Blue appliances serve small businesses and offer a cheap device with multiple features.

This device offers two levels of administration full-admin and site-admin. Site admin offers reduced permissions and for example doesn't allow you to add new admin users or add network connections for VPN site to sites etc.. However site-admin lets the user save the current users list to a csv file and also reupload a users list. For those of you who are thinking it can't be that easy… yep it is!

Log into the Admin panel and under user accounts, CSV User lists click on Save user list



Below displays the contents of the saved file.

Find your user name copy and paste it back into the list. Change your username and then change siteadmin to admin. Save your file and reupload it using the Load user list option.

```
#user,plaintext-password,group,redirect,fileshare,webshare,admin-level,encrypted-password,engrypted-nt-password,encrypted-lanman-password


"local-admin","","open","","personal","","admin","5Oj5MLk9uJuOw","37D1083AD016401B764BC3FC6B82CD02","6F56DF2F7B3A409BAAD3B435B51404EE"
"local-admin1","","open","","personal","","siteadmin","5Oj5MLk9uJuOw","37D1083AD016401B764BC3FC6B82CD02","6F56DF2F7B3A409BAAD3B435B51404EE"
```

You now have full admin access on the soho blue/netpilot device. The passwords are also stored in MD5 which using any good online service you have a decent chance at reversing. Quick and Simple.

On two older NetPilot devices I found an account equiinet with a password of Ed1S0n which may or may not be useful for those people who do not have any admin access.