Samba vulnerabilities allow hackers to invade thousands of remote Linux computers

A 7-year-old vulnerability was found on Samba software, allowing an attacker to hack and control Linux and Unix computers remotely.

Samba is an open source software that runs on popular platforms, including Windows, Linux, Unix, IBM System 390 and OpenVMS. It allows users of non-Windows operating systems like GNU / Linux or macOS to share folders, files, and computers with Windows via SMB protocol.

The newly discovered remote code execution vulnerability (CVE-2017-7497) **affects all new versions since Samba 3.5.0** released on March 1, 2010. Samba wrote on his page on Wednesday:

> All Samba versions from 3.5.0 and later have a remote code execution vulnerability, allowing infected clients to upload content to shared folders and cause the server to download and execute the file " .

Is this the Linux version of the EternalBlue vulnerability?

According to the Shodan search engine, more than 485,000 Samba installation computers use port 445 to access the Internet. According to researchers at Rapid 7, **more than 104,000 endpoints on the Internet run Samba versions with vulnerabilities, of which 92,000 endpoints run unsupported Samba versions** .

Picture 1 of Samba vulnerabilities allow hackers to invade thousands of remote Linux computers

Since Samba is the SMB protocol used on Linux and Unix systems, some experts think it is the EternalBlue Linux version, the vulnerability is exploited by WannaCry. Should we call this SambaCry?

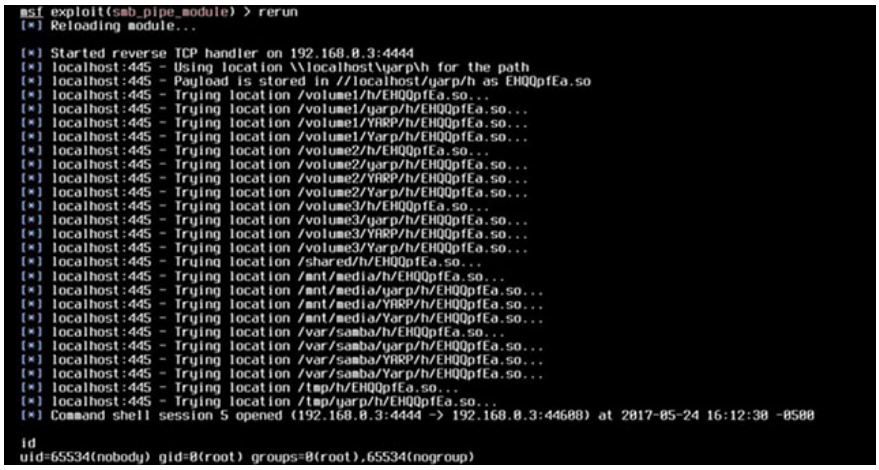
Keep in mind that the number of systems with vulnerabilities is numerous and the exploitation of vulnerabilities is also very easy, **Samba can completely create a large-scale attack** . Even Home Network private networks can be exploited if used with devices with network attached storage (NAS).

Exploiting code (using Metasploit tool)

This vulnerability is exploited through the way Samba shares files. The attacker uses the random Samba module to upload to the public folder and when the user server downloads it, it will execute the malicious code. Exploiting the vulnerability is very simple, just a piece of code to execute the malicious code on the infected machine.

simple.create_pipe ("/ path / to / target.so")

The Samba vulnerability has been put on Metasploit (a framework used to test, using code that exploits vulnerabilities), allowing researchers and hackers to easily exploit the vulnerability.



Patch

Samba patched for new versions 4.6.4, 4.5.10 and 4.4.14. Users of the Samba version of the vulnerability are still encouraged to quickly install the patch. If you can't update the latest versions of Samba immediately, you can avoid this vulnerability by adding the following line to Samba's smb.conf file.

nt pipe support = no

After adding, you only need to restart the SMB daemon (smbd). This will prevent the client from accessing the network and disable some functions to connect to Windows.

Although publishers of Linux distributions, including Red Hat and Ubuntu, have released patches for users, the threat still comes from NAS devices when they cannot be updated quickly. Craig Williams of Cisco said that because most NAS devices run Samba and contain important data, this vulnerability has "the *risk of becoming the first large-scale ransomware worm on Linux* ".

Meanwhile, NETGEAR also offers security advice regarding CVE-2017-7494, that many routers and NAS products have been affected by using Samba version 3.5.0 or higher. However, the company has just released an update guide for ReadyNAS products running OS 6.x.