CVE Exploit

OS Exploitation- (CVE-2011-2523)

vsftpd 2.3.4- Backdoor Command Execution with Manual and Metasploit Examples

Ransika A.A.P.W.R.Y

- **Vulnerability Assessment Report:** VSFTPD 2.3.4 Backdoor Exploitation
- **Date:** October 27, 2023
- **Subject:** Unauthorized Command Execution Vulnerability in VSFTPD Version 2.3.4

----

1. Introduction

File Transfer Protocol (FTP) servers are quintessential for the transfer of files across the internet. One such FTP server, the Very Secure FTP Daemon (VSFTPD), is known for its claim of being the most secure FTP server available. However, a specific version of this software, version 2.3.4 (available for download between June 30, 2011, and July 3, 2011), was found to contain a malicious backdoor. This vulnerability allows attackers to execute unauthorized commands by opening a shell on port 6200/tcp.

2. Discovery

The malicious backdoor in VSFTPD 2.3.4 was identified and reported publicly on July 4, 2011. This revelation was shocking for many in the cybersecurity community, given the reputation of VSFTPD for its security features.

3. Technical Description

The root of this vulnerability lies in a clandestine backdoor intentionally embedded within the VSFTPD 2.3.4 software. When exploited, this backdoor opens a shell on port 6200/tcp. This grants the attacker unauthorized access to execute commands on the compromised system. The presence of such a backdoor in a widely-used FTP server poses a significant risk, especially for systems that remain unpatched.

4. Exploitation

Following the public disclosure of this vulnerability, multiple exploits were developed to leverage this backdoor:

1. Nmap Scripting Engine (NSE): An Nmap script named 'ftp-vsftpd-backdoor' was developed, which tests systems for the presence of the VSFTPD 2.3.4 backdoor. By default, this script uses the benign 'id' command to test the vulnerability. However, with specific script arguments, attackers can execute any desired command.

2.Python Exploit Script: A more direct method, a Python exploit script, was made available for this vulnerability. When executed, this script can compromise VSFTPD 2.3.4 systems by exploiting the backdoor, underlining the critical risk this vulnerability poses.

❖Exploitation using Metasploit Framework

Step 1: Metasploit Framework Initialization:

- Open a terminal in your sever
- Launch the Metasploit console by entering msfconsole in the terminal.
  - ➢ ***msfconsole***

Step 2: Local Network Configuration:

- Obtain the local IP configuration by executing ifconfig within the Metasploit console.
- Repeat the ifconfig command in a separate Kali Linux terminal to confirm network settings.
  - ➢ ***ifconfig***

Step 3: Network Scanning:

- Conduct a comprehensive port scan using nmap targeting the Metasploit machine's IP address with the command: nmap [Metasploit_IP_address] -p- -sV -vv. This identifies open ports and services running on the Metasploit machine.
    - ➢ ***nmap [target Ip address] -p- -sV -vv***

Step 4: Vulnerability Identification:

- Utilize searchsploit, a command-line search tool for Exploit Database, to search for exploits related to vsFTPd 2.3.4 by executing searchsploit vsftpd 2.3.4.
    - ➢ ***searchsploit vsftpd 2.3.4***

Step 5: Exploit Selection:

- In the Metasploit console, search for vsFTPd 2.3.4 related exploits using search vsftpd 2.3.4.
    - ➢ ***search for vsFTPd 2.3.4***

- Select the appropriate exploit module with the command: use 0 (assuming this is the index for unix/ftp/vsftpd_234_backdoor).
    - ➢ ***Use 0(unix/ftp/vsftpd_234_backdoor)***

Step 6: Exploit Configuration:

- Display the current configuration and required settings for the selected exploit by running show options.
    - ➢ ***show options***

- Configure the exploit by setting the remote host IP address with the command: set RHOSTS [target_ip_address].

- ***set RHOSTS [target_ip_address]***

- Verify all options are set correctly with another show options command.

Step 7: Exploitation Execution:

- Launch the exploit using run or exploit command. If successful, this should open a backdoor connection to the target system running vsFTPd 2.3.4.
  - ***run or exploit***

Step 8: Post-Exploitation:

- The report should also include a section on post-exploitation, including any access gained, data retrieved, and further actions taken. It is crucial to reiterate the importance of ethical hacking practices and legal compliance.

❖Exploitation using Python Exploit Script

Step 1: Requirements and Installation

- Python3 and its package manager pip were installed:
  - ***sudo apt install python3 python3-pip***

- The argparse library, necessary for parsing command-line arguments, was installed via pip:
  - ***pip install argparse***

Step 2: Installation of the Exploit

- The exploit code was cloned from a GitHub repository:
  - ***git clone https://github.com/padsalatushal/CVE-2011-2523.git***

- The cloned directory was accessed, and execution permissions were granted to the exploit script:
  - ***cd CVE-2011-2523***
  - ***chmod +x exploit.py***

Step 3: Exploitation Process

- The exploit was initiated by running the Python script with the target host's IP address:
  - ***python3 exploit.py -host Target_IP***

----

5. Verification

To ascertain whether a particular system is vulnerable to this backdoor, one can utilize the aforementioned tools:

- The Nmap NSE script provides a quick and efficient method for systems administrators and penetration testers to scan their networks for vulnerable VSFTPD installations.
- Alternatively, the Python exploit script can be used for a more hands-on verification, especially in controlled testing environments.

6. Mitigation

Upon discovery of the backdoor, the development team behind VSFTPD took immediate action. The vulnerability was addressed, and a patched version, 2.3.5-3, was released. Systems administrators are strongly advised to:

- Upgrade their VSFTPD installations to version 2.3.5-3 or later.
- Regularly monitor official channels and cybersecurity bulletins for any updates or patches.
- Implement network monitoring to detect any suspicious activities, especially on port 6200/tcp.

7. Conclusion

The discovery of the backdoor in VSFTPD 2.3.4 serves as a reminder of the ever-present threats in the digital realm. While the vulnerability posed a significant security risk, the swift response in patching the software and the availability of tools to detect vulnerable systems has mitigated potential damage. Organizations must remain vigilant, continuously monitor their digital assets, and ensure that they are using the latest, patched software versions to safeguard against such threats.

References

1. CVEdetails.com: CVE-2011-2523

2. CVE.mitre.org: CVE-2011-2523

3. Nmap Scripting Engine documentation: ftp-vsftpd-backdoor NSE script

4. Vulmon: Python exploit for vsftpd 2.3.4

5. ResearchGate: Exploiting Vulnerabilities of a Linux Based Machine: Penetration

END
