

# vsftpd 2.3.4 Vulnerability Remediation Document

---

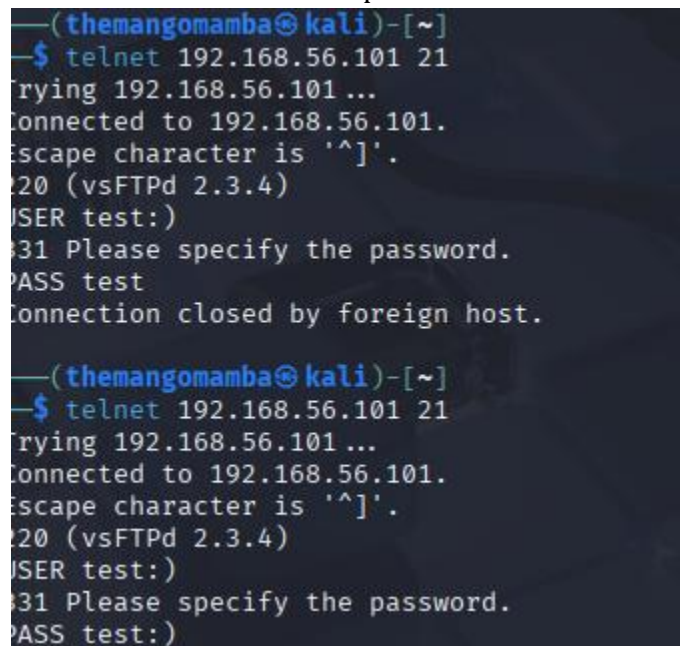
## Vulnerability Summary

CVE-2011-2523 affects vsftpd version 2.3.4. A malicious backdoor was introduced into this release, allowing attackers to gain remote root access. The backdoor is triggered when a specially crafted username containing the characters ':' is submitted, which causes a shell to open on TCP port 6200. Successful exploitation leads to complete system compromise, exposing sensitive data and allowing attackers to move laterally within the network.

## Systems Affected

Any system running vsftpd version 2.3.4 is vulnerable, particularly Linux servers configured with this version of the FTP daemon. Test environments such as Metasploitable 2 include the vulnerable service for training purposes, but production servers running this version are at risk. Systems exposing FTP on port 21 without network segmentation or firewall restrictions are especially vulnerable to exploitation.

Evidence of exploitation and remediation steps are documented with screenshots, including service identification and exploit execution.



```
(themangomamba@kali)-[~]
$ telnet 192.168.56.101 21
Trying 192.168.56.101...
Connected to 192.168.56.101.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
USER test:)
331 Please specify the password.
PASS test
Connection closed by foreign host.

(themangomamba@kali)-[~]
$ telnet 192.168.56.101 21
Trying 192.168.56.101...
Connected to 192.168.56.101.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
USER test:)
331 Please specify the password.
PASS test:)
```

## Mitigation Steps

The most effective mitigation is to upgrade vsftpd to a secure version such as 2.3.5 or later. Administrators should also remove or block access to the backdoor port 6200 using firewall rules, and restrict FTP access to trusted IP addresses only. Beyond the FTP service, it is important to apply all pending patches to system packages to eliminate other potential entry points. Reviewing user accounts and system logs for evidence of suspicious activity is also necessary to detect prior compromise.

## Verification Steps

Once patched, administrators should confirm that vsftpd is running a secure version. FTP login should be tested with legitimate user accounts to ensure the backdoor is no longer triggered. A network scan using a tool like Nmap should verify that TCP port 6200 is closed, and log files should be checked for any signs of unexpected shell connections or other anomalies.

## Ongoing Security Measures

To prevent similar issues in the future, organizations should enable automatic updates for critical packages, schedule regular vulnerability scans across their infrastructure, and implement monitoring and alerting systems to detect unusual login attempts or suspicious network connections. Finally, maintaining proper network segmentation ensures that if one service is compromised, the impact is limited and attackers cannot freely pivot through the environment.