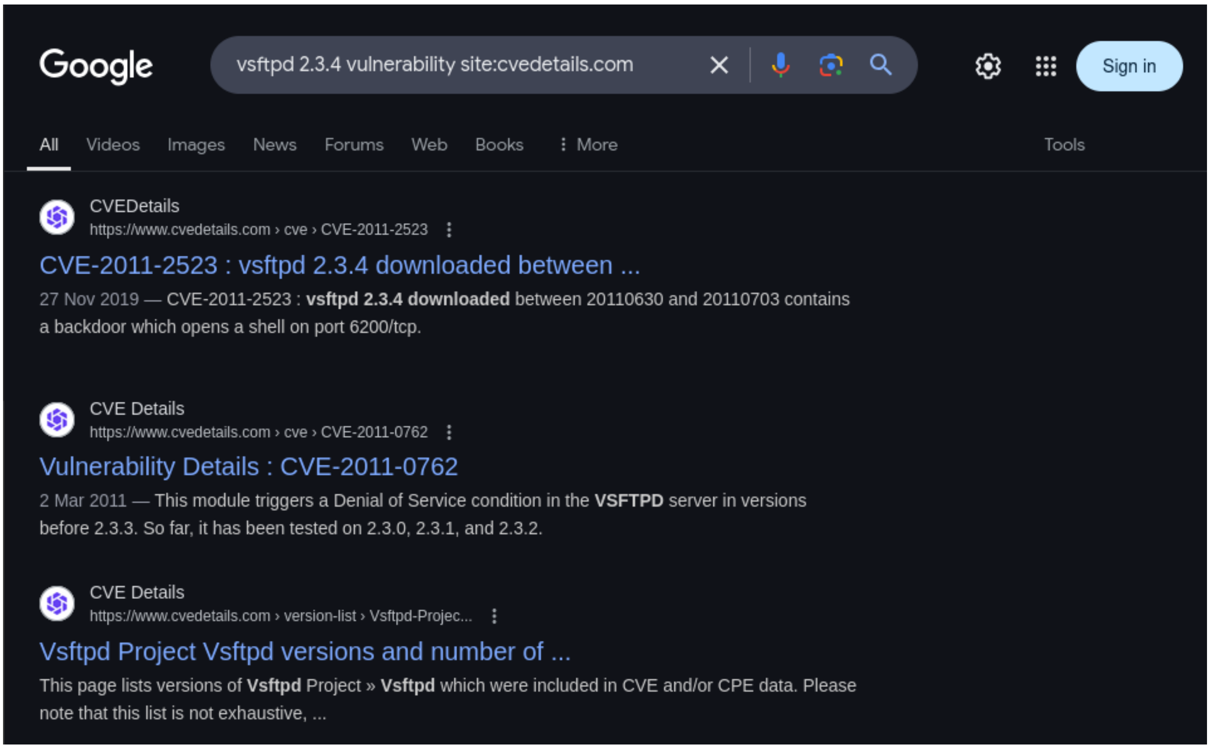
Task 2: Vulnerability Research with Google Dorking

1. Find vulnerabilities related the port using its version. We found this using the '–sC -sV' flags with nmap.



Google
vsftpd 2.3.4 vulnerability site:cvedetails.com
Sign in
All Videos Images News Forums Web Books ⋮ More Tools

CVEDetails
https://www.cvedetails.com › cve › CVE-2011-2523

CVE-2011-2523 : vsftpd 2.3.4 downloaded between ...

27 Nov 2019 — CVE-2011-2523 : **vsftpd 2.3.4 downloaded** between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

CVE Details
https://www.cvedetails.com › cve › CVE-2011-0762

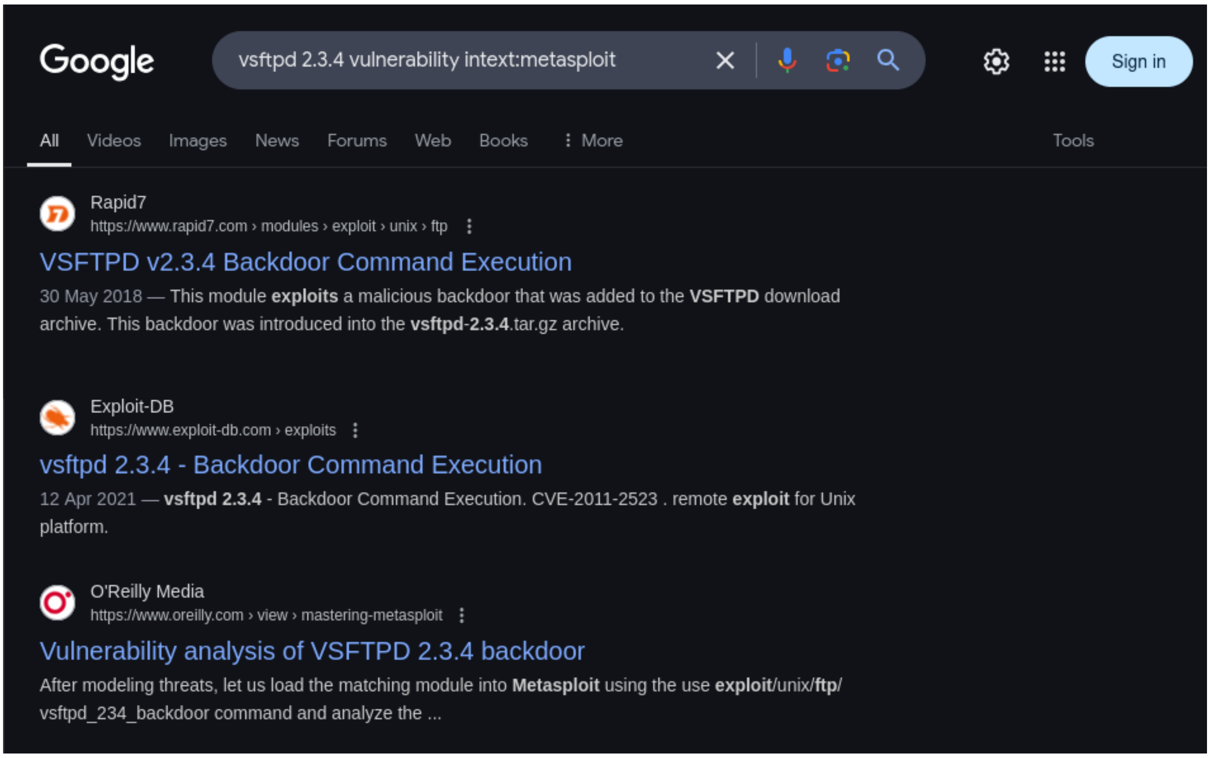
Vulnerability Details : CVE-2011-0762

2 Mar 2011 — This module triggers a Denial of Service condition in the **VSFTPD** server in versions before 2.3.3. So far, it has been tested on 2.3.0, 2.3.1, and 2.3.2.

CVE Details
https://www.cvedetails.com › version-list › Vsftpd-Projec...

Vsftpd Project Vsftpd versions and number of ...

This page lists versions of **Vsftpd** Project » **Vsftpd** which were included in CVE and/or CPE data. Please note that this list is not exhaustive, ...



Google
vsftpd 2.3.4 vulnerability intext:metasploit
Sign in
All Videos Images News Forums Web Books ⋮ More Tools

Rapid7
https://www.rapid7.com › modules › exploit › unix › ftp

VSFTPD v2.3.4 Backdoor Command Execution

30 May 2018 — This module **exploits** a malicious backdoor that was added to the **VSFTPD** download archive. This backdoor was introduced into the **vsftpd-2.3.4**.tar.gz archive.

Exploit-DB
https://www.exploit-db.com › exploits

vsftpd 2.3.4 - Backdoor Command Execution

12 Apr 2021 — **vsftpd 2.3.4** - Backdoor Command Execution. CVE-2011-2523 . remote **exploit** for Unix platform.

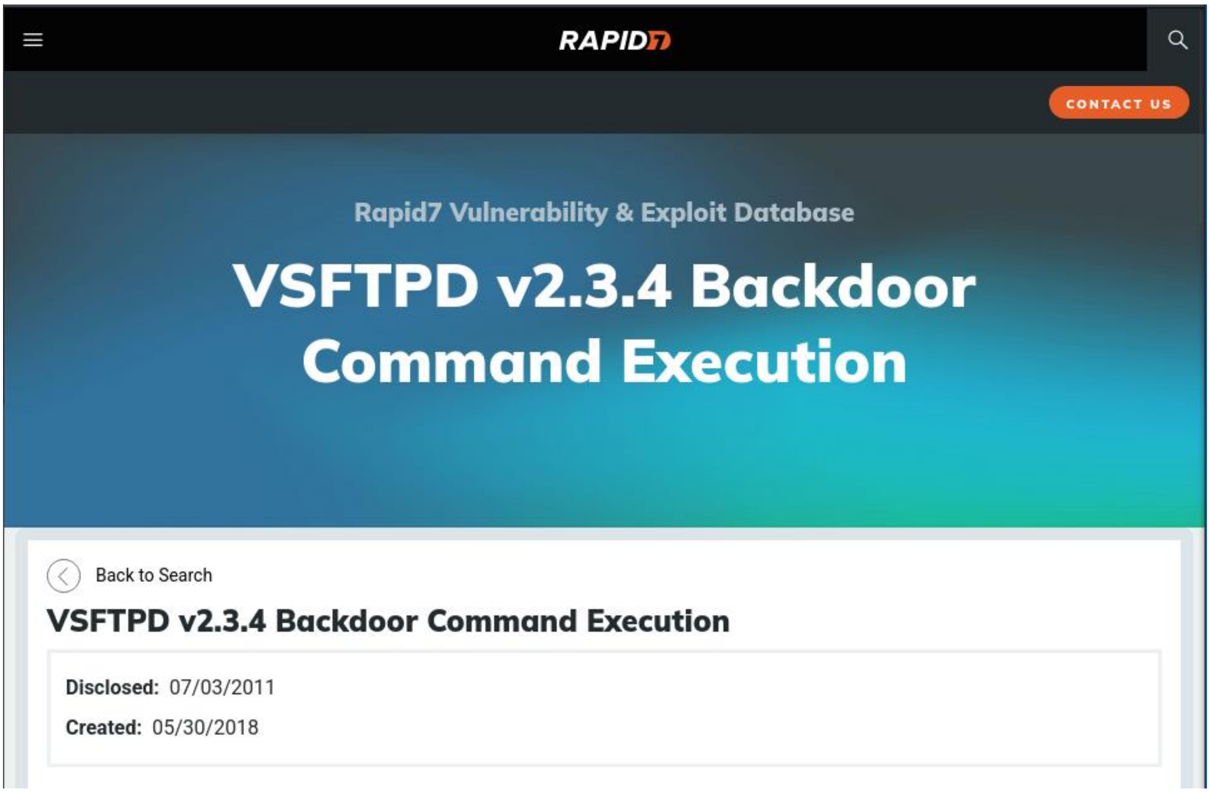
O'Reilly Media
https://www.oreilly.com › view › mastering-metasploit

Vulnerability analysis of VSFTPD 2.3.4 backdoor

After modeling threats, let us load the matching module into **Metasploit** using the use **exploit**/unix/**ftp**/vsftpd_234_backdoor command and analyze the ...

NOTE: Using 'site' we can force the search engine to return websites from cvedetails.com only. There is also 'filetype' (specify the filetype) and 'intext' (filters searches that use the specified word).

2. Using the search results display what you have learned



Rapid7 Vulnerability & Exploit Database

VSFTPD v2.3.4 Backdoor Command Execution

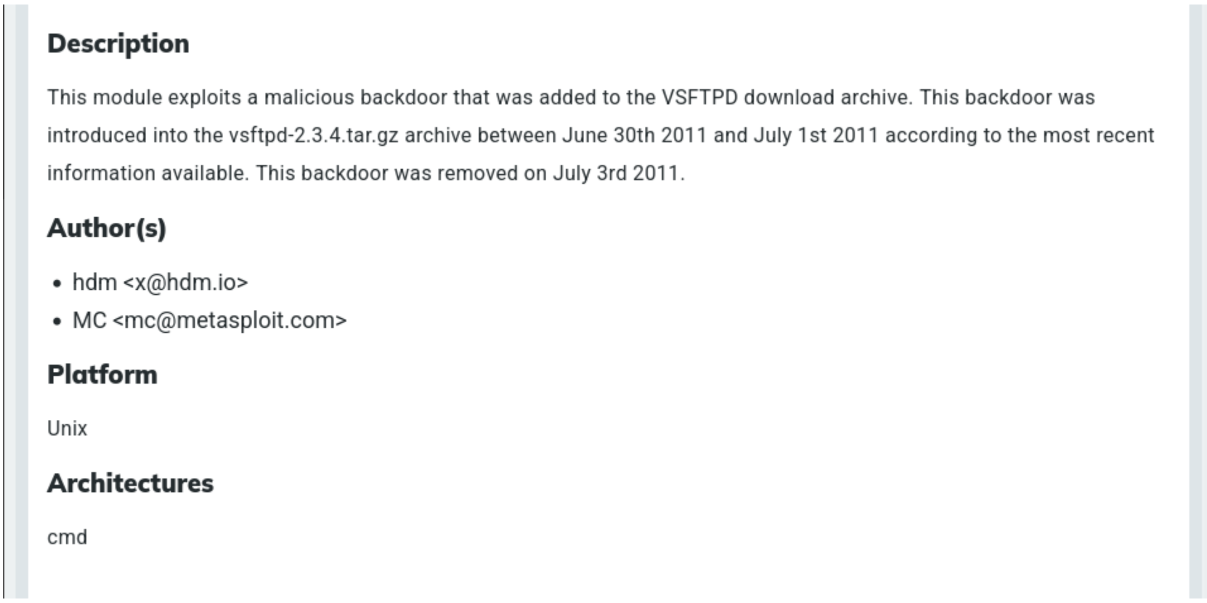
Back to Search

VSFTPD v2.3.4 Backdoor Command Execution

Disclosed: 07/03/2011

Created: 05/30/2018

NOTE: We can see that VSFTPD has been disclosed in 2011. It is very old and potentially outdated.



Description

This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.

Author(s)

- hdm <x@hdm.io>
- MC <mc@metasploit.com>

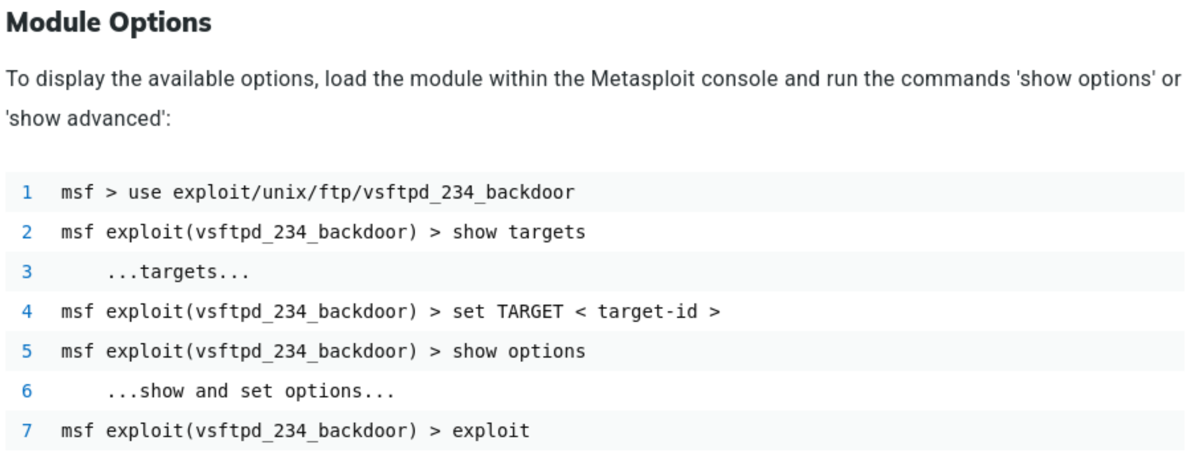
Platform

Unix

Architectures

cmd

NOTE: Scrolling down we can see a description for a exploit for this model, the authors involved, platform and what architectures are used.



Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show targets
    ...targets...
msf exploit(vsftpd_234_backdoor) > set TARGET < target-id >
msf exploit(vsftpd_234_backdoor) > show options
    ...show and set options...
msf exploit(vsftpd_234_backdoor) > exploit
```

NOTE: Finally, we can see that a Metasploit module exists for this vulnerability, and it includes the steps to use it.

NOTE: Exploit DB is another website that provides a vulnerability database. It includes the backend code of an exploit that takes advantage of the service version. This can be used to do manual exploitation if the Metasploit module doesn’t work.

Conclusion:

- Sites like exploit.db and rapid7 are powerful tools when it comes to vulnerability research
- Google Dorking is an effective way to enhance searching capabilities