# CVE-2015-1701

## What is CVE

The acronym CVE represents "Common Vulnerabilities and Exposures." It is a system for locating, characterizing, and classifying known vulnerabilities and exposures in hardware and software related to information security. The main goal of the CVE system is to provide vulnerabilities and exposures a standard designation, which will facilitate information sharing and coordination between security experts and businesses as they work to mitigate these threats.

Every CVE entry has a distinct CVE identifier, which takes the form "CVE-YYYY-NNNNN." The identifier consists of a sequential number and the year. An example of a specific vulnerability or exposure found in 2023 is "CVE-2023-12345".The CVE Program, formerly run by MITER Corporation, maintains a database containing CVE entries, which are available to the general public. These entries can also be found on a number of websites and databases pertaining to cybersecurity and vulnerabilities. A CVE entry generally comprises the following: a description of the vulnerability or exposure; details on the hardware or software products that are impacted; the seriousness of the issue; and links to more information or patches that can assist businesses in mitigating the issue.

In conclusion, CVE is an essential part of the cybersecurity environment because it offers a defined and well-recognized technique for locating, monitoring, and controlling security exposures and vulnerabilities. Because it makes it possible to systematize the reporting and resolution of security issues, it is essential to maintaining the security of hardware and software systems.

# CVE-2015-1701 Introduction

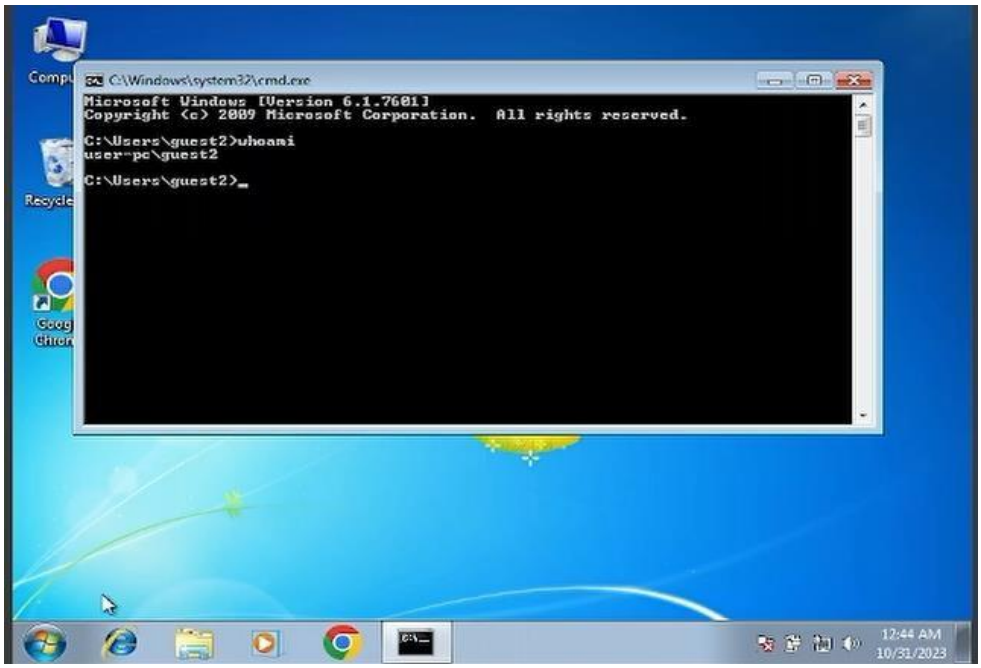
Recently, FireEye Labs discovered a limited APT operation that took advantage of zero-day vulnerabilities in Microsoft Windows and Adobe Flash. FireEye analysts used the Dynamic Threat Intelligence Cloud (DTI) to identify a pattern of attacks that started on April 13, 2015. Adobe independently fixed APSB15-06's vulnerability (CVE-20153043). Based on the analysis of command-and-control infrastructure and technical indicators, FireEye determines that APT28 is most likely the party responsible for this activity.

The Windows local privilege escalation vulnerability (CVE-2015-1701) is known to Microsoft. Although a fix for the Windows vulnerability is not yet available, this in-the-wild attack can be neutralized by updating Adobe Flash to the most recent version. Only the combination of CVE2015-1701 and the Adobe Flash exploit for CVE-2015-3043 has been observed in use. The Microsoft Security Team is working on a fix for CVE-2015-1701.

# Methodology and Results

1.

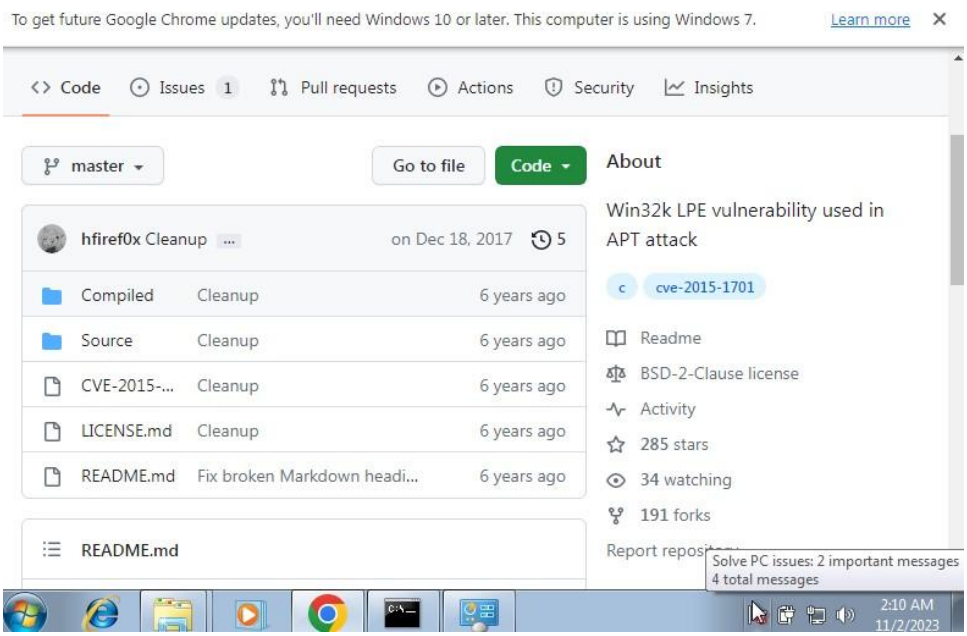
For this exploit, we had to use one virtual machine, we had to install Windows 7 into our oracle vm VirtualBox. Open the windows 7 virtual machine. Then enter a cmd on the windows 7 machine and enter the "whoami" to get the machine 7 IP Address. The whoami command is a simple command used in command-line interfaces, including Unix-like operating systems (such as Linux) and Windows. When you run the whoami command, it returns the username of the currently logged-in user.



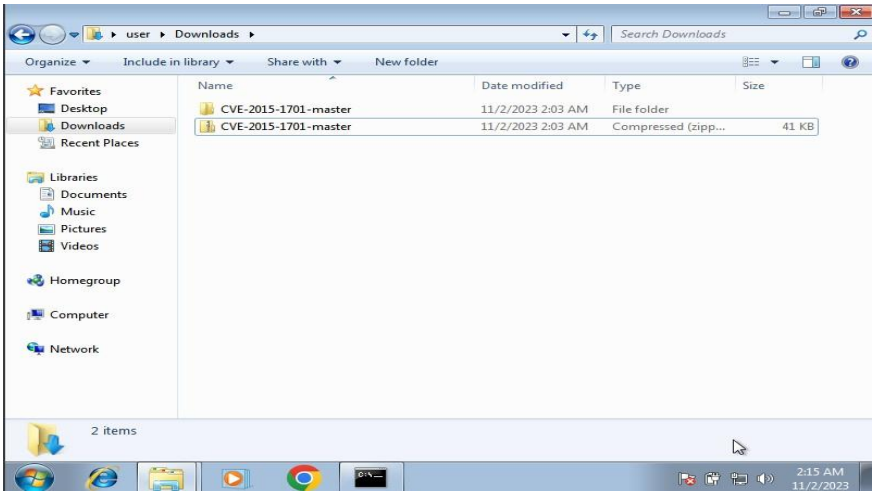

2.

Go to Google and type CVE-2015-1701 github. Download the github code.

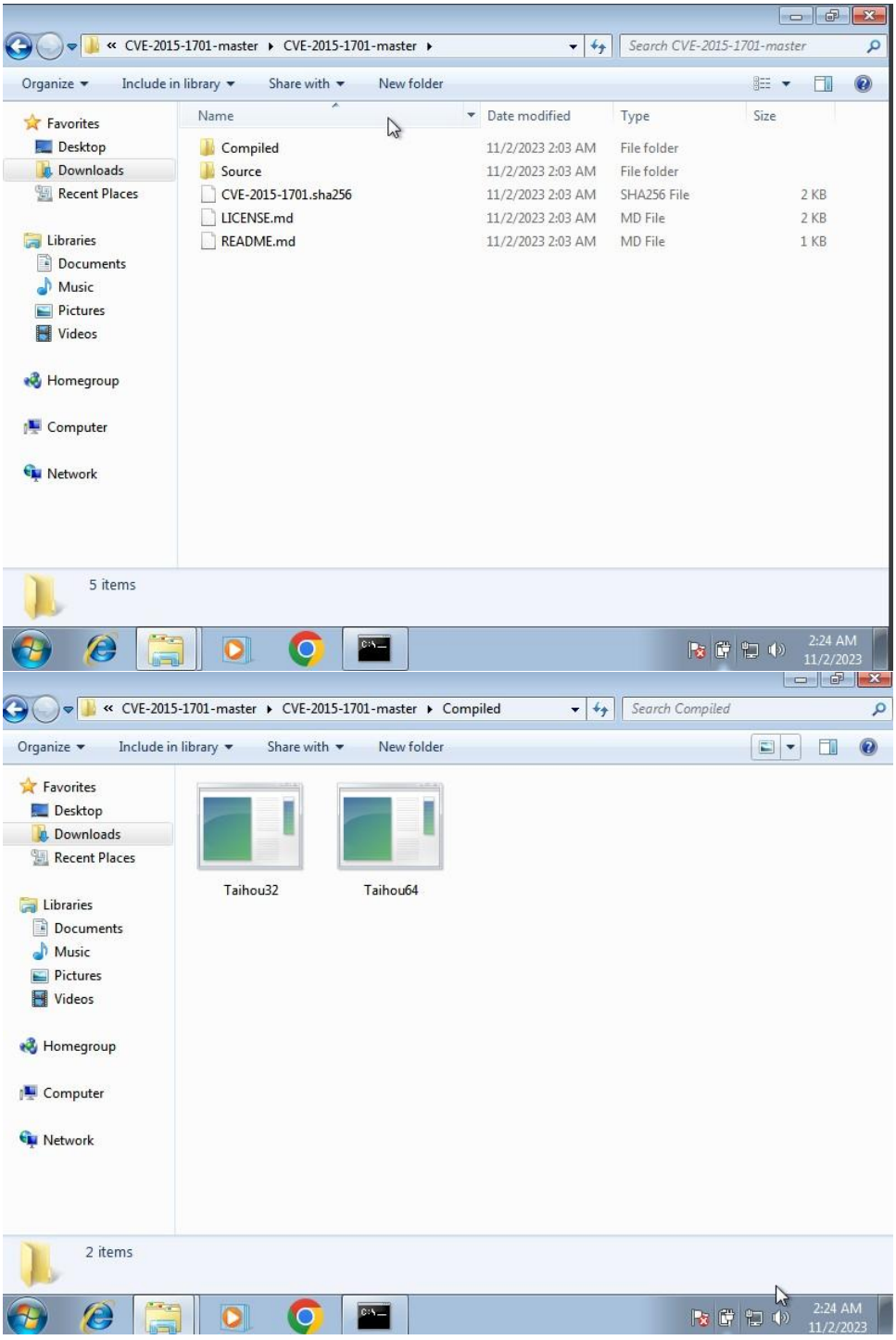
Link - https://github.com/hfiref0x/CVE-2015-1701




3. Go to the download folder and extract it.

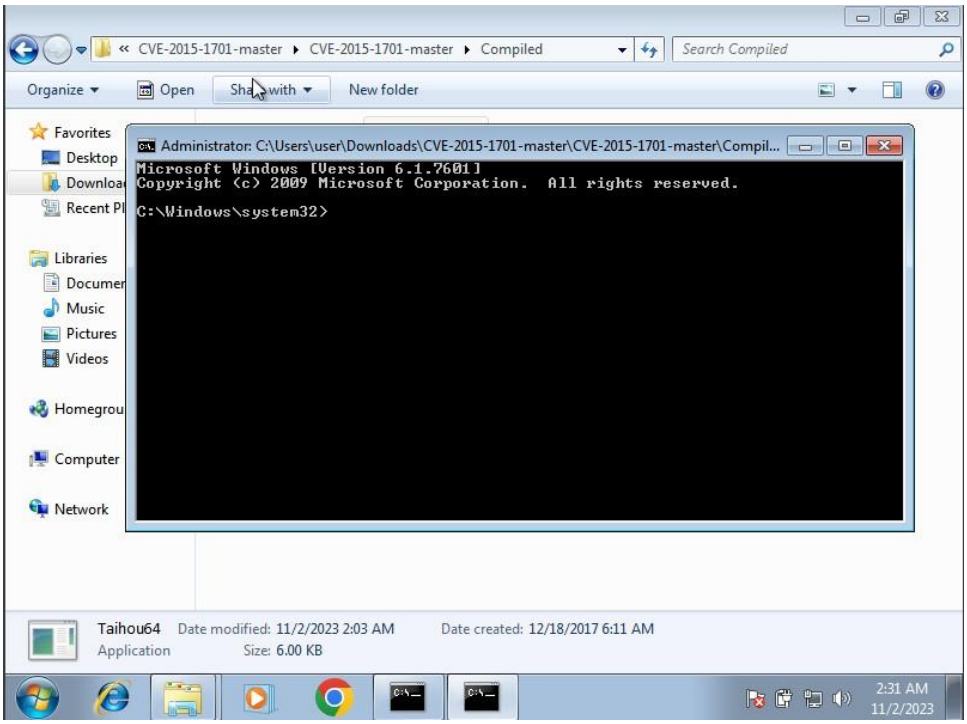



4. Enter the extract folder. After entering the compiled folder, you will see two files. Depending on the opening system, you can select this file and double-click on the selected file.


« CVE-2015-1701-master ▸ CVE-2015-1701-master ▸
Search CVE-2015-1701-master
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
Name
Date modified
Type
Size
Compiled 11/2/2023 2:03 AM File folder
Source 11/2/2023 2:03 AM File folder
CVE-2015-1701.sha256 11/2/2023 2:03 AM SHA256 File 2 KB
LICENSE.md 11/2/2023 2:03 AM MD File 2 KB
README.md 11/2/2023 2:03 AM MD File 1 KB
5 items
2:24 AM
11/2/2023
« CVE-2015-1701-master ▸ CVE-2015-1701-master ▸ Compiled
Search Compiled
Taihou32
Taihou64
2 items
2:24 AM
11/2/2023

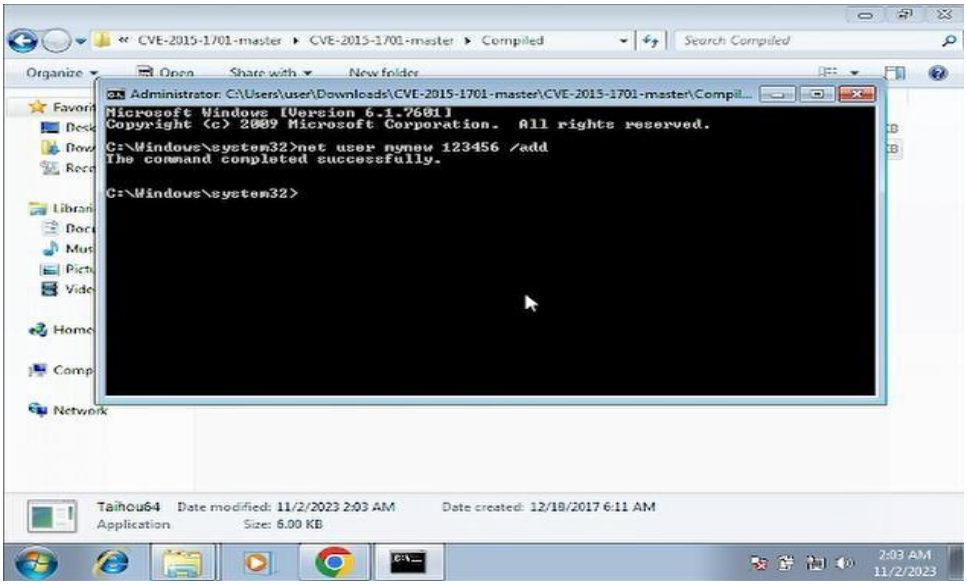
5.

After double click, we bypass user privilege directory administrator privilege.



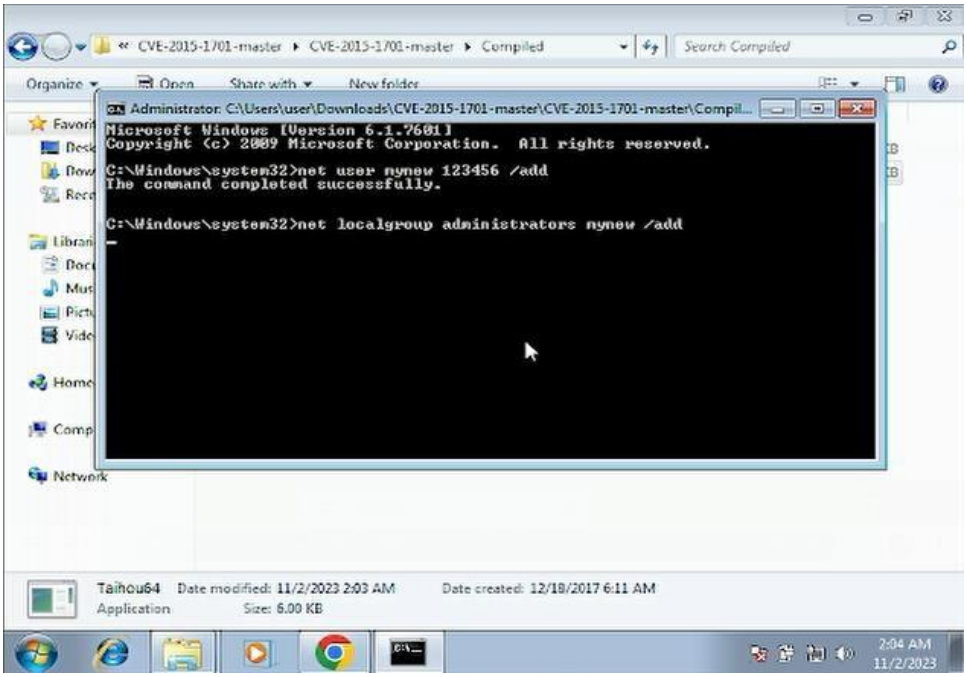

6.

Next type "net user [account name] [password] /add" and enter. Then you can see that the command is running successfully



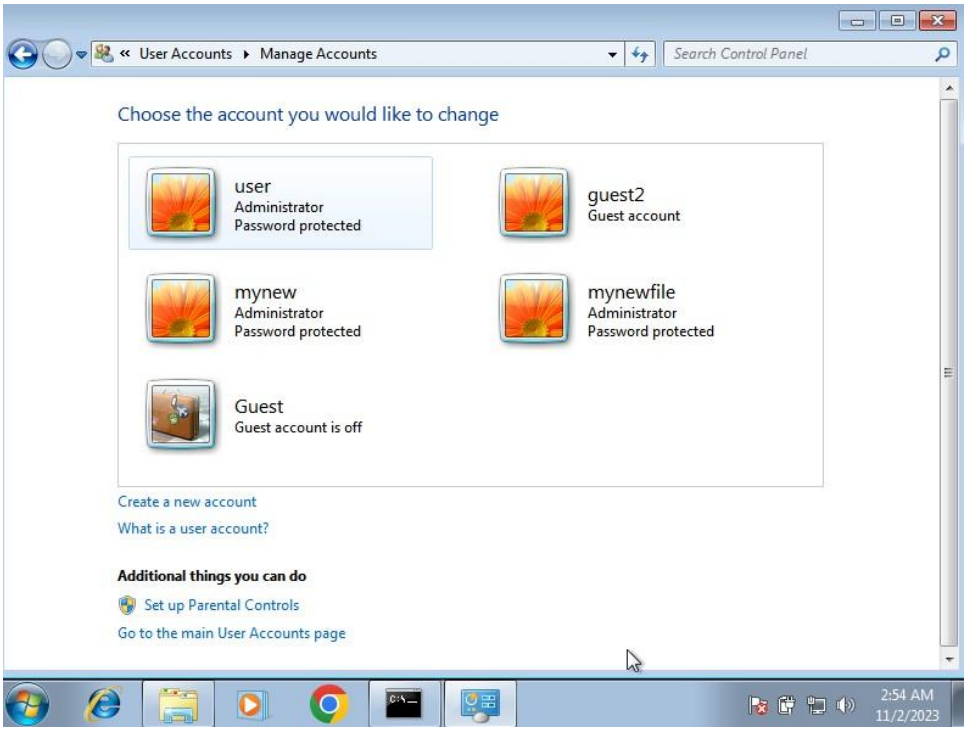
7.

Next, convert the user account to an administrator account. So, type "net localgroup administrators mynew /add" and enter.




8.

We have done everything successfully. go back to the control panel. Click user account and family safety. Then click add or remove user account. we can see all the information add or remove user account. We can see my new file has complete administrator privilege right now.


« User Accounts ▸ Manage Accounts
Search Control Panel
Choose the account you would like to change
user
Administrator
Password protected
guest2
Guest account
mynew
Administrator
Password protected
mynewfile
Administrator
Password protected
Guest
Guest account is off
Create a new account
What is a user account?
Additional things you can do
Set up Parental Controls
Go to the main User Accounts page
2:54 AM
11/2/2023