LAB 14: VULNERABILITY ASSESSMENT

Class M02 student ID b2014926 Name Tran Dang Khoa

1. Design your scenario of vulnerability assessment

No	Steps	Remarks
1	Environment setting	Inspection area: Network vulnerable Target: Ubuntu 14.04, Firefox, 172.19.128.128 Attacker: Virtual machine, Kali Linux, Firefox, (bridged adapter)
2	Choose one scanning model	B: Nmap vulners
	Install scanning program	git clone https://github.com/vulnersCom/nmap-vulners.git
3	Run the program	sudo nmap -sV --script vulners.nse 172.19.128.128
4	Analyze the result based on your idea	List up the vulnerability checking items Grade the vulnerability level

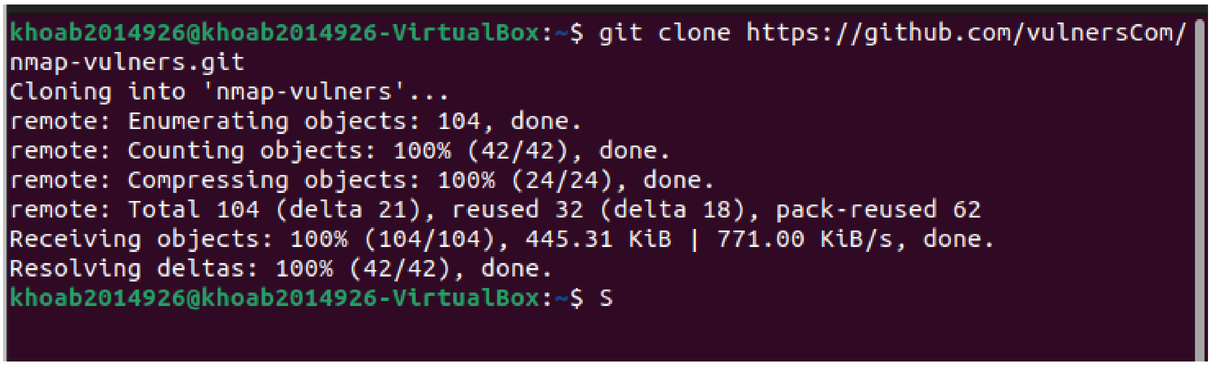
2. Exercise the following vulnerability assessment process

No	Steps	Remarks
1	Environment Setting	1 Inspection area Network, Web vulnerable 2 Target: Ubuntu 14.04, Firefox, 172.19.128.128 3 Attacker: Kali Linux, Firefox, 172.19.128.22
2	**Choose scanning program/tool**	**Nmap vulners**

3	**Set the scanning environment, command**	**Input target address on program/tool** **Set the scanning options:** -sV --script vulners.nse 172.19.128.128
4	**Execute the scanning program**	**Run the scanning program:** **sudo nmap -sV --script vulners.nse 172.19.128.128**
5	**Print out scanning result**	
6	**Analyze the result based on your idea**	Grade the vulnerability level: - As we can have seen from the results above, the target machine vulnerability level is really high: 9 or 10 Explain the analyzing result: - After running the program the script will look up records from several vulnerability database such as CVE, National Vulnerability, … to check and link the public vulnerability from the results of nmap.

3. Explain your scenario

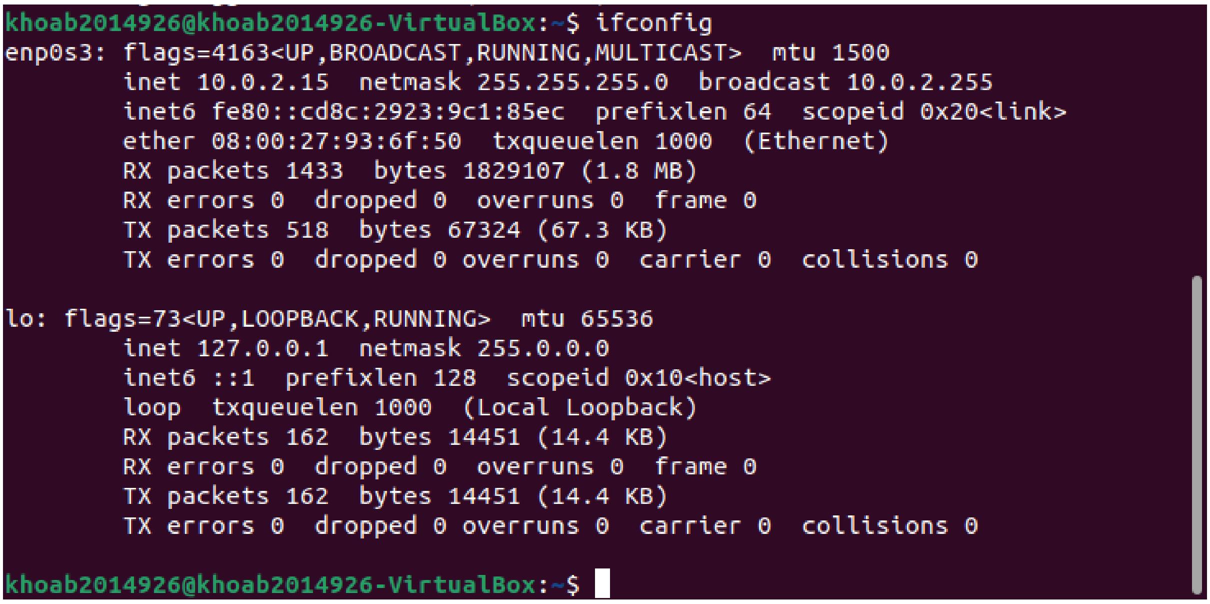
-Download if from Github:



```
khoab2014926@khoab2014926-VirtualBox:~$ git clone https://github.com/vulnersCom/
nmap-vulners.git
Cloning into 'nmap-vulners'...
remote: Enumerating objects: 104, done.
remote: Counting objects: 100% (42/42), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 104 (delta 21), reused 32 (delta 18), pack-reused 62
Receiving objects: 100% (104/104), 445.31 KiB | 771.00 KiB/s, done.
Resolving deltas: 100% (42/42), done.
khoab2014926@khoab2014926-VirtualBox:~$ S
```

- Check the network information

  Target

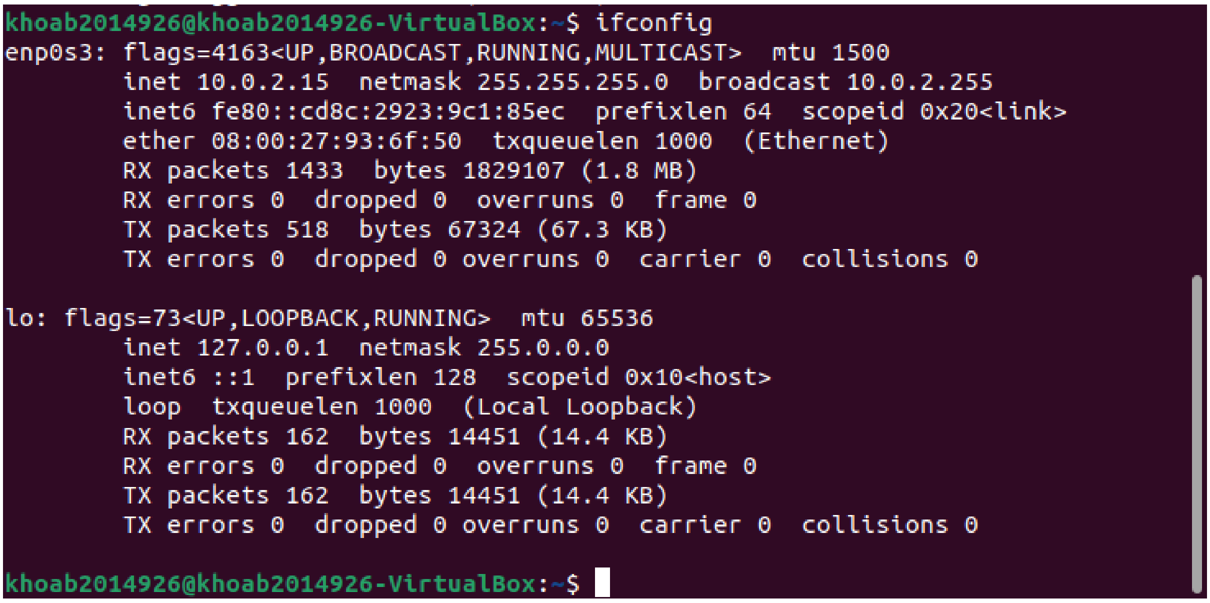


```
khoab2014926@khoab2014926-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::cd8c:2923:9c1:85ec  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:93:6f:50  txqueuelen 1000  (Ethernet)
        RX packets 1433  bytes 1829107 (1.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 518  bytes 67324 (67.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 162  bytes 14451 (14.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 162  bytes 14451 (14.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

khoab2014926@khoab2014926-VirtualBox:~$ 
```

Attacker

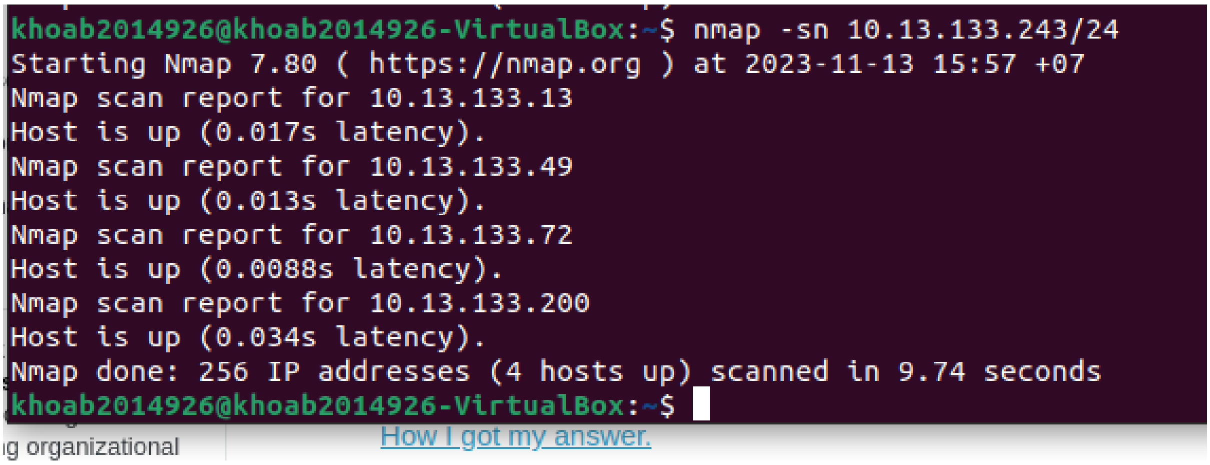


```
khoab2014926@khoab2014926-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::cd8c:2923:9c1:85ec  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:93:6f:50  txqueuelen 1000  (Ethernet)
        RX packets 1433  bytes 1829107 (1.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 518  bytes 67324 (67.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 162  bytes 14451 (14.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 162  bytes 14451 (14.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

khoab2014926@khoab2014926-VirtualBox:~$ 
```

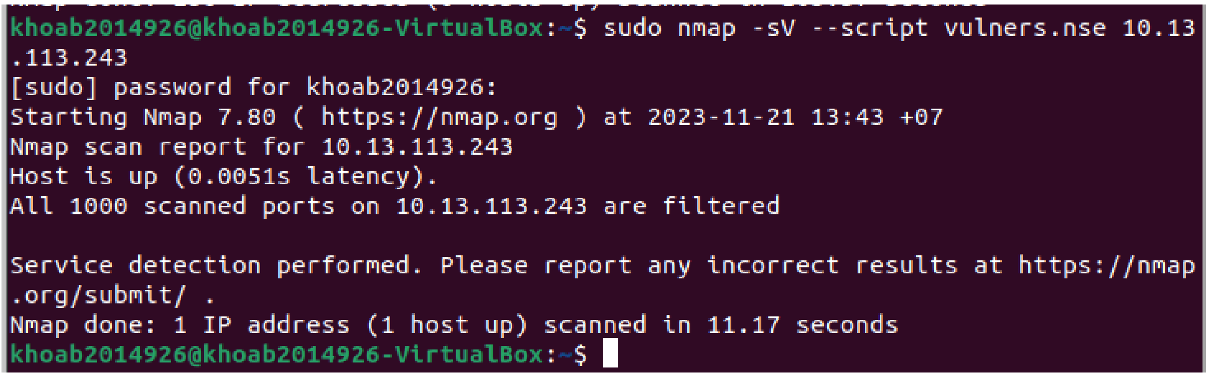
- Running nmap to discover open host in the network



```
khoab2014926@khoab2014926-VirtualBox:~$ nmap -sn 10.13.133.243/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-13 15:57 +07
Nmap scan report for 10.13.133.13
Host is up (0.017s latency).
Nmap scan report for 10.13.133.49
Host is up (0.013s latency).
Nmap scan report for 10.13.133.72
Host is up (0.0088s latency).
Nmap scan report for 10.13.133.200
Host is up (0.034s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 9.74 seconds
khoab2014926@khoab2014926-VirtualBox:~$
```

- ıg organizational How I got my answer.

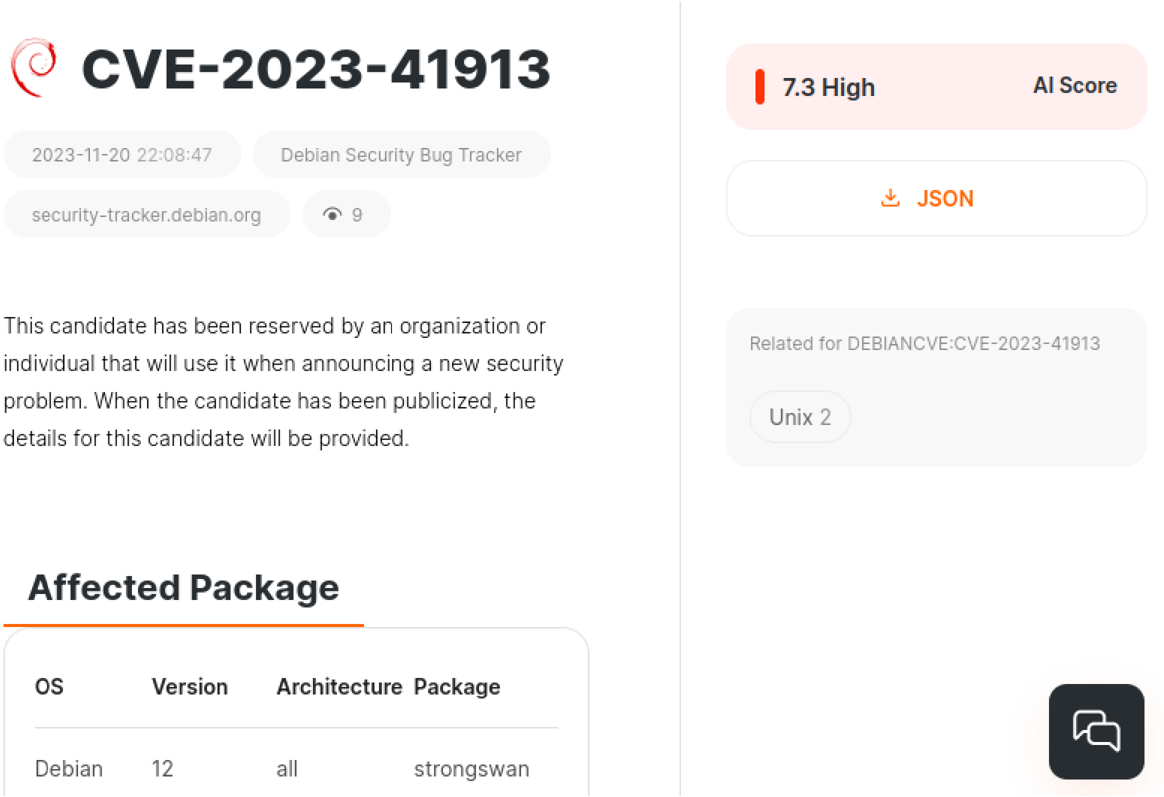
- See there are a lot of vulnerabilities in the target machince about FTP, SSH, HTTP, IPP



```
khoab2014926@khoab2014926-VirtualBox:~$ sudo nmap -sV --script vulners.nse 10.13
.113.243
[sudo] password for khoab2014926:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-21 13:43 +07
Nmap scan report for 10.13.113.243
Host is up (0.0051s latency).
All 1000 scanned ports on 10.13.113.243 are filtered

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.17 seconds
khoab2014926@khoab2014926-VirtualBox:~$
```

CVE-2023-41913



CVE-2023-41913

2023-11-20 22:08:47

Debian Security Bug Tracker

security-tracker.debian.org

9

This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

7.3 High AI Score

JSON

Related for DEBIANCVE:CVE-2023-41913

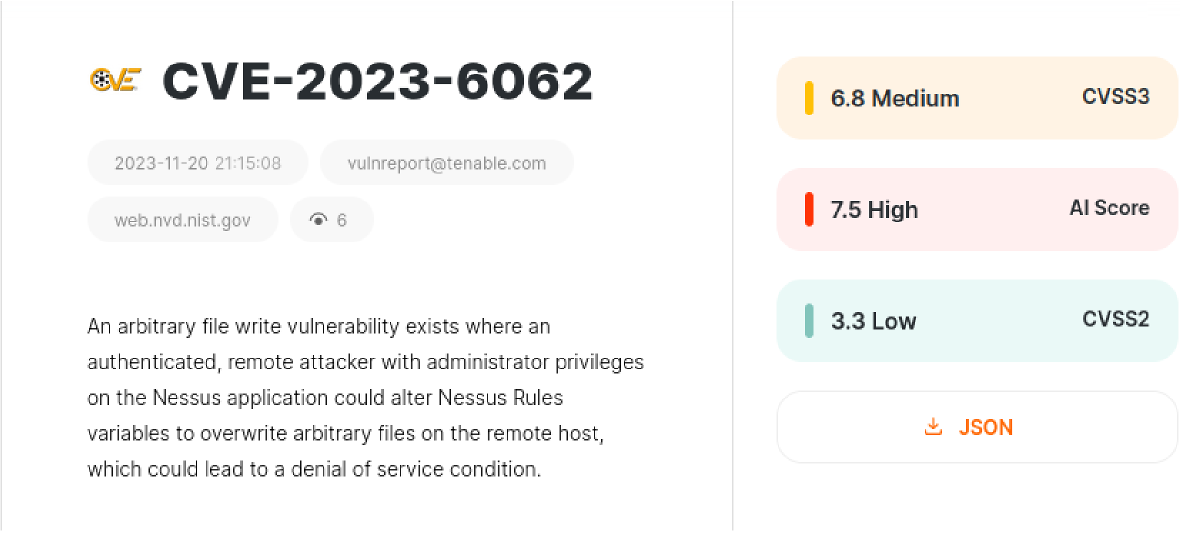
Unix 2

Affected Package

OS	Version	Architecture	Package
Debian	12	all	strongswan

This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2023-6062



CVE-2023-6062

2023-11-20 21:15:08

vulnreport@tenable.com

web.nvd.nist.gov

6

An arbitrary file write vulnerability exists where an authenticated, remote attacker with administrator privileges on the Nessus application could alter Nessus Rules variables to overwrite arbitrary files on the remote host, which could lead to a denial of service condition.

6.8 Medium CVSS3

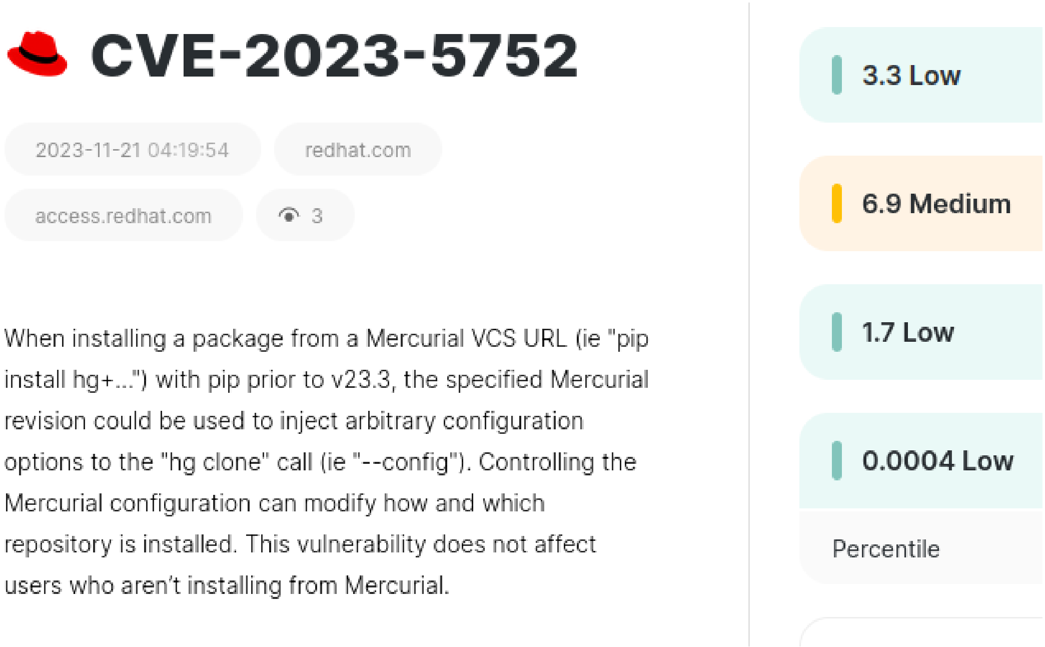
7.5 High AI Score

3.3 Low CVSS2

JSON

An arbitary file write vulnerability exists where an authenticated, remote attacker with administrator privileges on the Nessus application could alter Nessus Rules variables to overwrite arbitrary files on the remote host which could lead to a denial of service condition.

CVE-2023-5752



CVE-2023-5752

2023-11-21 04:19:54

redhat.com

access.redhat.com

3

When installing a package from a Mercurial VCS URL (ie "pip install hg+...") with pip prior to v23.3, the specified Mercurial revision could be used to inject arbitrary configuration options to the "hg clone" call (ie "--config"). Controlling the Mercurial configuration can modify how and which repository is installed. This vulnerability does not affect users who aren't installing from Mercurial.

3.3 Low

6.9 Medium

1.7 Low

0.0004 Low

Percentile

When installing a package from a Mercurial VCS URL (ie “pip install hg+…”)

With pip prior to v23.3, the specified Mercurial revision could be used to inject arbitrary configuration options to the “hg clone” call (ie “—config”). Controlling the Mercurial configuration can modify how and which repository is installed. This vulnerability does not affect users who aren’t installing from Mecurial>