

CSIS Advisory

Outlook Email File Attachment Denial of Service Vulnerability

Document written and evaluated by:

Sarid Harper

sha@csis.dk



Technical report

Publish date: november 26, 2010

Contents

1	Summary	3
2	Affected Versions	3
3	Screen-dumps	3
4	Resolution	4
5	Time-line	4
6	Credits	4
7	References	4

1 Summary

A vulnerability has been discovered in Outlook, which can be exploited by malicious, anonymous individuals to cause a DoS (Denial of Service).

The vulnerability is caused as a result of the improper handling of email file attachments with no extension. This can be exploited to cause a DoS by tricking a user into clicking on an attachment with no file extension in the reading pane.

2 Affected Versions

This vulnerability is confirmed in the following version:

- Microsoft Outlook 2007 (12.0.6539.5000) SP2 MSO (12.0.6545.5004)

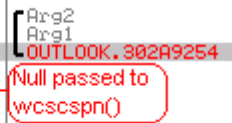
Other versions may also be affected.

3 Screen-dumps

<pre> 00 DB 00 00 DB 00 55 PUSH EBP 8BEC MOV EBP,ESP 8B40 08 MOV ECX, DWORD PTR SS:[Arg1] 0FB701 MOVZX EAX, WORD PTR DS:[ECX] 56 PUSH ESI 33F6 XOR ESI,ESI 66:85C0 TEST AX,AX 74 46 JE SHORT 302A92AB 0FB7C0 MOVZX EAX,AX 83F8 2E CMP EAX,2E 0F84 91A5E5FF JE 301A3802 83F8 3F CMP EAX,3F 0F84 79A5E5FF JE 301A37F3 83F8 5C CMP EAX,5C 75 02 JNE SHORT 302A9281 33F6 XOR ESI,ESI 41 INC ECX 41 INC ECX 0FB701 MOVZX EAX, WORD PTR DS:[ECX] 66:85C0 TEST AX,AX 75 DA JNE SHORT 302A9265 85F6 TEST ESI,ESI 74 1C JE SHORT 302A92AB 8BC6 MOV EAX,ESI 8D50 02 LEA EDX,[EAX+2] 66:8B08 MOV CX, WORD PTR DS:[EAX] 40 INC EAX 40 INC EAX 66:85C9 TEST CX,CX 75 F6 JNE SHORT 302A9294 2BC2 SUB EAX,EDX D1F8 SAR EAX,1 74 07 JE SHORT 302A92AB 8BC6 MOV EAX,ESI 5E POP ESI 5D POP EBP C2 0800 RETN 8 33C0 XOR EAX,EAX </pre>	<pre> OUTLOOK.302A9254(guessed Arg1,Arg2) Path to attachment Move first byte to eax, zero the rest Save esi Clear esi Do we have anything in a1? Do we have a '.'? Do we have a '?'? Do we have a '\'? Next char in path to attachment Again (Unicode) Move next char into eax, zero rest Got something? The extension, if it exists, is in eax </pre>
--	---

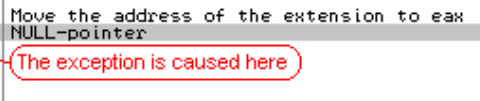
```

0F85 0E682C01 JNE 30794C66
53          PUSH EBX
56          PUSH ESI
E8 F5ADD0FF CALL 302A9254
8BF8      MOV EDI,EAX
68 9CFE9230 PUSH 3092FE9C
57          PUSH EDI
FF15 B4110031 CALL DWORD PTR DS:[&MSUCR80.wcscspn]
    
```



```

C3          RETN
8B4424 04   MOV EAX,DWORD PTR SS:[ESP+4]
66:8338 00   CMP WORD PTR DS:[EAX],0
53          PUSH EBX
56          PUSH ESI
57          PUSH EDI
74 2B     JE SHORT 78180AEF
    
```



4 Resolution

Turn off the reading pane.

5 Time-line

1. Vulnerability identified: 03.09.10
2. Vendor informed: 19.11.10
3. Vendor response: 24.11.10
4. Vendor fix: Currently unavailable

6 Credits

Vulnerability identified by Sarid Harper of the CSIS Security Group.

7 References

Turn the Reading Pane off or on:

http://office.microsoft.com/en-us/outlook-help/make-changes-to-the-reading-preview-pane-HA010118503.aspx?CTT=1#_Toc267389729