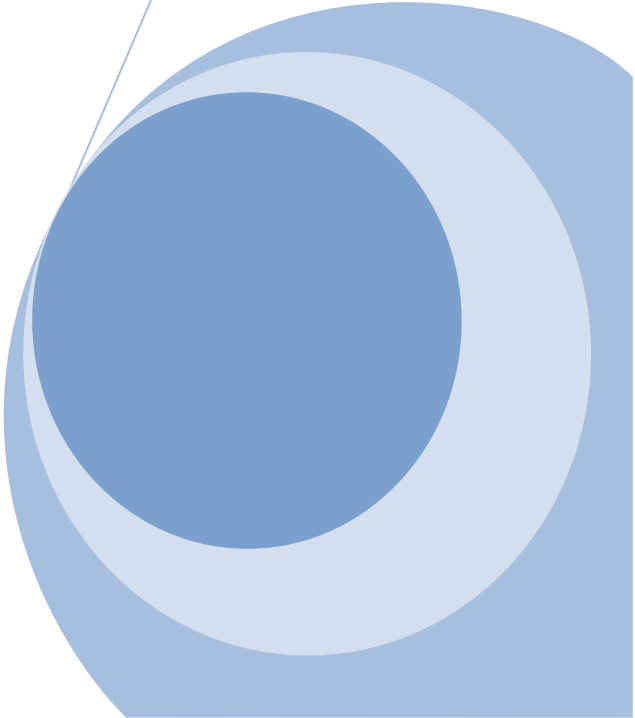
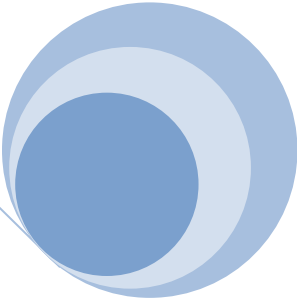
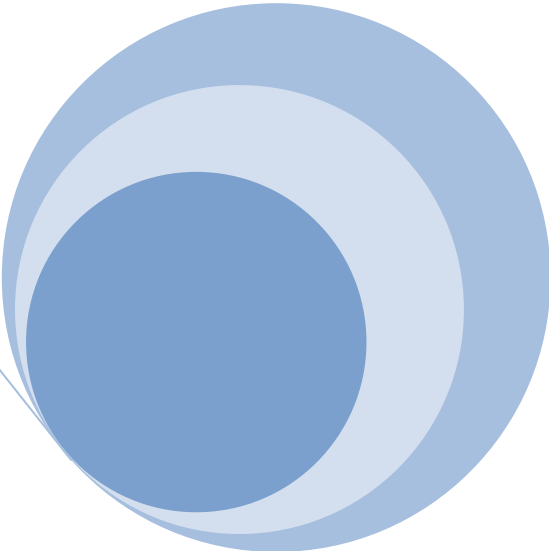


# Cabri 3d by Apuromafo

CLS  
[29-4-11]



Saludos, hace un tiempo escribí sobre la version 1.2.x y veamos si variado en la nueva versión **Cabri 3D 2.1.2**.

Greetings, in some time was writed about 1.2 version and now are a new version **Cabri 3D 2.1.2**

00404FD6	51	PUSH ECX	
00404FD7	E8 E4BD0000	CALL Cabri_3D.00410DC0	
00404FDC	8AD8	MOV BL,AL	
00404FDE	83C4 0C	ADD ESP,0C	
00404FE1	84DB	TEST BL,BL	
00404FE3	8B5C24 22	MOV BYTE PTR SS:[ESP+22],BL	
00404FE7	0F85 EA000000	JNZ Cabri_3D.004050D7	
00404FED	8D9424 A40000	LEA EDX,DWORD PTR SS:[ESP+A4]	
00404FF4	52	PUSH EDX	
00404FF5	8D8C24 F00000	LEA ECX,DWORD PTR SS:[ESP+F0]	
00404FFC	FF15 38414100	CALL DWORD PTR DS:[&MSUCP71.std::basic_string<wchar_t,std::char_traits<	msvcop71.std::basic_string<wchar_t,std::char_traits<
00405002	B3 0A	MOV BL,0A	
00405004	68 E8514100	PUSH Cabri_3D.004151E8	Unicode "\etc\license.cg3"
00405009	8D8C24 F00000	LEA ECX,DWORD PTR SS:[ESP+F0]	
00405010	8B9C24 BC0900	MOV BYTE PTR SS:[ESP+9BC],BL	
00405017	FF15 88404100	CALL DWORD PTR DS:[&MSUCP71.std::basic_string<wchar_t,std::char_traits<	msucop71.std::basic_string<wchar_t,std::char_traits<

img Tute anterior/img old tute

1 call , etc\license.cg3 y cmp c/ 8

Referencias Actuales/Actually Ref.:

0040501D	PUSH Cabri_3D.004193F0	Unicode "Creating application "
0040507F	PUSH Cabri_3D.004193DC	Unicode "clipboard"
0040521F	PUSH Cabri_3D.004193B8	Unicode "\etc\license.cg3"
004052A9	PUSH Cabri_3D.004193B0	Unicode "box"
004055A1	PUSH Cabri_3D.00419368	Unicode "rd registration error"

pequeños cambios con al/bl, la misma cmp con 8 / are little changes with al/bl, same cmp with 8



004051F3	51	PUSH ECX	
004051F4	E8 C7FF0000	CALL Cabri_3D.004151C0	
004051F9	83C4 0C	ADD ESP,0C	
004051FC	84C0	TEST AL,AL	
004051FE	8B4424 22	MOV BYTE PTR SS:[ESP+22],AL	
00405202	0F85 03010000	JNZ Cabri_3D.0040530B	
00405208	8D9424 C00000	LEA EDX,DWORD PTR SS:[ESP+C0]	
0040520F	52	PUSH EDX	
00405210	8D8C24 B00000	LEA ECX,DWORD PTR SS:[ESP+B0]	
00405217	FF15 7C004100	CALL DWORD PTR DS:[&MSUCP71.??0?\$basic_string@WU?\$c	MSUCP71.??0?\$basic_string@WU?\$c
0040521D	B3 0A	MOV BL,0A	
0040521F	68 B8934100	PUSH Cabri_3D.004193B8	Unicode "\etc\license.cg3"
00405224	8D8C24 B00000	LEA ECX,DWORD PTR SS:[ESP+B0]	
0040522B	8B9C24 BC0900	MOV BYTE PTR SS:[ESP+9BC],BL	
00405232	FF15 14814100	CALL DWORD PTR DS:[&MSUCP71.?append0?\$	MSUCP71.?append0?\$basic_string@_
00405238	8B8424 C40000	MOV EAX,DWORD PTR SS:[ESP+C4]	
0040523F	BD 00000000	MOV EBP,8	
00405244	3BC5	CMP EAX,EBP	
00405246	8B8424 B00000	MOV EAX,DWORD PTR SS:[ESP+B0]	
0040524D	73 07	JNB SHORT Cabri_3D.00405256	
0040524F	8D8424 B00000	LEA EAX,DWORD PTR SS:[ESP+B0]	
00405256	> 50	PUSH EAX	

En call = 3 llamadas, tambien pueden ser forzadas. //3 calls as same old, and can be forced

004151B7	CALL	INT3	
004151C0	83EC 10	SUB ESP,10	Local calls from 004051F4, 0040526C, 0040AB65
004151C3	56	PUSH ESI	
004151C4	8B7424 18	MOV ESI,DWORD PTR SS:[ESP+18]	
004151C8	57	PUSH EDI	
004151C9	8D4424 08	LEA EAX,DWORD PTR SS:[ESP+8]	
004151CD	50	PUSH EAX	
004151CE	56	PUSH ESI	
004151CF	E8 CCFEFFFF	CALL Cabri_3D.004150A0	
004151D4	83C4 08	ADD ESP,8	
004151D7	8DBE 04040000	LEA EDI,DWORD PTR DS:[ESI+404]	
004151DD	33D2	XOR EDX,EDX	
004151DF	B9 04000000	MOV ECX,4	
004151E4	8D7424 08	LEA ESI,DWORD PTR SS:[ESP+8]	
004151E8	F3:A7	REPE CMPS DWORD PTR ES:[EDI],DWORD PTR I	
004151EA	8BC2	MOV EAX,EDX	
004151EC	5F	POP EDI	
004151ED	0F94C0	SETE AL	
004151F0	5E	POP ESI	
004151F1	83C4 10	ADD ESP,10	
004151F4	C3	RETN	
004151F5	CC	INT3	

SETE AL -> setne Al, cambiando desde sete al a setne al, veamos si es igual a la v. 1.2.x //

SETE AL -> setne Al changing from sete al to setne al, check if are same that 1.2.x version:

 <b>Cabri 3D 2.1.2</b> Plug-in 2.1.2	 <b>Cabri 3D 2.1.2</b> Plug-in 2.1.2
Concepción, arquitectura: Eric Bainville y Jean-Marie Laborde. Desarrollo y calidad: equipo Cabrilog. © 2004-2007 Cabrilog - Todos los derechos reservados.	Design, architecture: Eric Bainville and Jean-Marie Laborde. Development and Software Quality: Cabrilog. © 2004-2007 Cabrilog - All rights reserved.
<a href="#">Créditos</a>	<a href="#">Credits</a>
Licencia concedida .	Licensed to .

es igual/ is same

Conclusión

1 letter thinking in the past, can see that are the same place vulnerable// end.

Una hoja pensando en el pasado, puedo ver esta el mismo lugar vulnerable //fin.



saludos Apuromafo