

SatOri Advisory

SATA020110

Crimson Editor

Summary

A vulnerability has been discovered in Crimson Editor, which can be exploited by malicious, anonymous individuals to compromise a vulnerable system.

The vulnerability is caused as a result of improper bounds checking when reading words from dictionary files. This can be exploited to cause a stack-based buffer overflow by tricking a user into using a maliciously constructed dictionary file.

Successful exploitation of this vulnerability enables execution of arbitrary code.

Affected Versions

This vulnerability is confirmed in the following versions:

- Crimson Editor SVN263 English
- Crimson Editor 3.70 Release (Freeware)

Other versions may also be affected.

Screen-dumps

00334A38 MOV EDI, DWORD PTR DS:[EAX]
00334A39 DEC EDI
00334A3A CMP [ARG_1], EBX
00334A3B JNZ SHORT MSUCIRT.00334A4A
00334A3C MOV EAX, DWORD PTR DS:[ESI]
00334A3D MOV EAX, DWORD PTR DS:[EAX+4]
00334A3E LEA EAX, DWORD PTR DS:[EAX+ESI+8]
00334A3F OR DWORD PTR DS:[EAX], 2
00334A40 JMP SHORT MSUCIRT.00334A85
00334A41 TEST EDI, EDI
00334A42 JBE SHORT MSUCIRT.00334A8C
00334A43 MOV EAX, DWORD PTR DS:[ESI]
00334A44 MOV EAX, DWORD PTR DS:[EAX+4]
00334A45 MOV ECX, DWORD PTR DS:[EAX+ESI+4]
00334A46 CALL MSUCIRT.??sgetc@streambuf@@@QAEHXZ
00334A47 CMP EAX, -1
00334A48 JE SHORT MSUCIRT.00334A8E
00334A49 PUSH EAX
00334A4A CALL DWORD PTR DS:[&msvort.isspace]
00334A4B TEST EAX, EAX
00334A4C POP ECX
00334A4D JNZ SHORT MSUCIRT.00334A4A
00334A4E MOV AL, BYTE PTR SS:[EBP-4]
00334A4F MOV ECX, [ARG_1]
00334A50 MOV BYTE PTR DS:[EBX+ECX], AL
00334A51 MOV EAX, DWORD PTR DS:[ESI]
00334A52 MOV EAX, DWORD PTR DS:[EAX+4]
00334A53 MOV ECX, DWORD PTR DS:[EAX+ESI+4]
00334A54 CALL MSUCIRT.??stosscc@streambuf@@@QAEHXZ
00334A55 INC EBX
00334A56 CMP EBX, EDI
00334A57 JB SHORT MSUCIRT.00334A4E

-- (A) If [eax] == 0 we end up with a big number:
-- Read DIC word
-- Perform check
-- Jump out if unable to read
isspace
-- Move byte to lower eax
-- ecx used as an index
-- ebx used as an offset
-- Copy byte to stack-based buffer
-- Compare with the huge number above (A)
-- Of course it's below

Jump is taken
00334A4E=MSUCIRT.00334A4E
MSUCIRT.??S lstream@@@QAEAAV0@PAD0Z+7C

Address	Hex dump	ASCII
0012F600	00 00 00 00 00 00 00 00
0012F601	41 41 41 41 41 41 41 41	AAAAAAAA
0012F602	41 41 41 41 41 41 41 41	AAAAAAAA
0012F603	41 41 41 41 41 41 41 41	AAAAAAAA
0012F604	41 41 41 41 41 41 41 41	AAAAAAAA
0012F605	41 41 41 41 41 41 41 41	AAAAAAAA
0012F606	41 41 41 41 41 41 41 41	AAAAAAAA
0012F607	41 41 41 41 41 41 41 41	AAAAAAAA
0012F608	41 41 41 41 41 41 41 41	AAAAAAAA
0012F609	41 41 41 41 41 41 41 41	AAAAAAAA
0012F60A	41 41 41 41 41 41 41 41	AAAAAAAA
0012F60B	41 41 41 41 41 41 41 41	AAAAAAAA
0012F60C	41 41 41 41 41 41 41 41	AAAAAAAA
0012F60D	41 41 41 41 41 41 41 41	AAAAAAAA
0012F60E	41 41 41 41 41 41 41 41	AAAAAAAA
0012F60F	41 41 41 41 41 41 41 41	AAAAAAAA
0012F610	41 41 41 41 41 41 41 41	AAAAAAAA
0012F611	41 41 41 41 41 41 41 41	AAAAAAAA
0012F612	41 41 41 41 41 41 41 41	AAAAAAAA
0012F613	41 41 41 41 41 41 41 41	AAAAAAAA
0012F614	41 41 41 41 41 41 41 41	AAAAAAAA
0012F615	41 41 41 41 41 41 41 41	AAAAAAAA
0012F616	41 41 41 41 41 41 41 41	AAAAAAAA
0012F617	41 41 41 41 41 41 41 41	AAAAAAAA
0012F618	41 41 41 41 41 41 41 41	AAAAAAAA
0012F619	41 41 41 41 41 41 41 41	AAAAAAAA
0012F61A	41 41 41 41 41 41 41 41	AAAAAAAA
0012F61B	41 41 41 41 41 41 41 41	AAAAAAAA
0012F61C	41 41 41 41 41 41 41 41	AAAAAAAA
0012F61D	41 41 41 41 41 41 41 41	AAAAAAAA
0012F61E	41 41 41 41 41 41 41 41	AAAAAAAA
0012F61F	41 41 41 41 41 41 41 41	AAAAAAAA
0012F620	41 41 41 41 41 41 41 41	AAAAAAAA
0012F621	41 41 41 41 41 41 41 41	AAAAAAAA
0012F622	41 41 41 41 41 41 41 41	AAAAAAAA
0012F623	41 41 41 41 41 41 41 41	AAAAAAAA
0012F624	41 41 41 41 41 41 41 41	AAAAAAAA
0012F625	41 41 41 41 41 41 41 41	AAAAAAAA
0012F626	41 41 41 41 41 41 41 41	AAAAAAAA
0012F627	41 41 41 41 41 41 41 41	AAAAAAAA
0012F628	41 41 41 41 41 41 41 41	AAAAAAAA
0012F629	41 41 41 41 41 41 41 41	AAAAAAAA
0012F62A	41 41 41 41 41 41 41 41	AAAAAAAA
0012F62B	41 41 41 41 41 41 41 41	AAAAAAAA
0012F62C	41 41 41 41 41 41 41 41	AAAAAAAA
0012F62D	41 41 41 41 41 41 41 41	AAAAAAAA
0012F62E	41 41 41 41 41 41 41 41	AAAAAAAA
0012F62F	41 41 41 41 41 41 41 41	AAAAAAAA
0012F630	41 41 41 41 41 41 41 41	AAAAAAAA
0012F631	41 41 41 41 41 41 41 41	AAAAAAAA
0012F632	41 41 41 41 41 41 41 41	AAAAAAAA
0012F633	41 41 41 41 41 41 41 41	AAAAAAAA
0012F634	41 41 41 41 41 41 41 41	AAAAAAAA
0012F635	41 41 41 41 41 41 41 41	AAAAAAAA
0012F636	41 41 41 41 41 41 41 41	AAAAAAAA
0012F637	41 41 41 41 41 41 41 41	AAAAAAAA
0012F638	41 41 41 41 41 41 41 41	AAAAAAAA
0012F639	41 41 41 41 41 41 41 41	AAAAAAAA
0012F63A	41 41 41 41 41 41 41 41	AAAAAAAA
0012F63B	41 41 41 41 41 41 41 41	AAAAAAAA
0012F63C	41 41 41 41 41 41 41 41	AAAAAAAA
0012F63D	41 41 41 41 41 41 41 41	AAAAAAAA
0012F63E	41 41 41 41 41 41 41 41	AAAAAAAA
0012F63F	41 41 41 41 41 41 41 41	AAAAAAAA
0012F640	41 41 41 41 41 41 41 41	AAAAAAAA
0012F641	41 41 41 41 41 41 41 41	AAAAAAAA
0012F642	41 41 41 41 41 41 41 41	AAAAAAAA
0012F643	41 41 41 41 41 41 41 41	AAAAAAAA
0012F644	41 41 41 41 41 41 41 41	AAAAAAAA
0012F645	41 41 41 41 41 41 41 41	AAAAAAAA
0012F646	41 41 41 41 41 41 41 41	AAAAAAAA
0012F647	41 41 41 41 41 41 41 41	AAAAAAAA
0012F648	41 41 41 41 41 41 41 41	AAAAAAAA
0012F649	41 41 41 41 41 41 41 41	AAAAAAAA
0012F64A	41 41 41 41 41 41 41 41	AAAAAAAA
0012F64B	41 41 41 41 41 41 41 41	AAAAAAAA
0012F64C	41 41 41 41 41 41 41 41	AAAAAAAA
0012F64D	41 41 41 41 41 41 41 41	AAAAAAAA
0012F64E	41 41 41 41 41 41 41 41	AAAAAAAA
0012F64F	41 41 41 41 41 41 41 41	AAAAAAAA
0012F650	41 41 41 41 41 41 41 41	AAAAAAAA
0012F651	41 41 41 41 41 41 41 41	AAAAAAAA
0012F652	41 41 41 41 41 41 41 41	AAAAAAAA
0012F653	41 41 41 41 41 41 41 41	AAAAAAAA
0012F654	41 41 41 41 41 41 41 41	AAAAAAAA
0012F655	41 41 41 41 41 41 41 41	AAAAAAAA

Multiple return addresses are overwritten as well as the SE further up the stack

7C944141 ntdll.7C944141
7C927784 RETURN to ntdll.7C927784 from ntdll.7C90E906

Resolution

Update to Crimson Editor SVN286

Timeline

- Vulnerability identified: 02.01.10
- Vendor informed: 25.03.10
- Vendor fix: 02.04.10

References

- <http://blog.sat0ri.com/?p=414>
- <http://www.crimsoneditor.com/>
- <http://forum.emeraldeditor.com/index.php?topic=361.0>