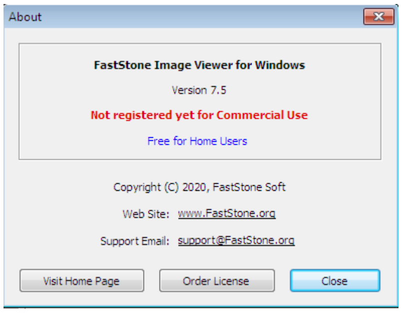
FastStone Image Viewer 7.5



About

FastStone Image Viewer for Windows

Version 7.5

Not registered yet for Commercial Use

Free for Home Users

Copyright (C) 2020, FastStone Soft

Web Site: www.FastStone.org

Support Email: support@FastStone.org

FastStone Image Viewer 7.5 has an out-of-bounds write (via a crafted image file) at FSViewer.exe+0x956e , 0xbe9c4, 0x96cf

CVE-2020-35843

The bug

eax=04040404 ebx=00015330 ecx=000001ba edx=0000000d esi=053e3b20 edi=0098c6ec

eip=0040956e esp=0018e594 ebp=0018e600 iopl=0 nv up ei pl nz na po nc

cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00010202

*** ERROR: Module load completed but symbols could not be loaded for image00400000

image00400000+0x956e:

0040956e 8938 mov dword ptr [eax],edi ds:002b:04040404=00650074

CVE-2020-35844

The bug

eax=003f15e0 ebx=000002b4 ecx=0278ba20 edx=00003400 esi=03bf696c edi=00d21da0

eip=004be9c4 esp=0018e210 ebp=0018e21c iopl=0 nv up ei pl zr na pe nc

cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00010246

*** WARNING: Unable to verify checksum for image00400000

*** ERROR: Module load completed but symbols could not be loaded for image00400000

image00400000+0xbe9c4:

004be9c4 8a0401 mov al,byte ptr [ecx+eax] ds:002b:02b7d000=??

CVE-2020-35845

The bug

eax=3b3bdf63 ebx=3b3bdf60 ecx=0018e5f0 edx=055213f0 esi=053e3b20 edi=00000000

eip=004096cf esp=0018e5fc ebp=0018e664 iopl=0 nv up ei pl nz na po nc

```
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00010202

*** WARNING: Unable to verify checksum for image00400000

*** ERROR: Module load completed but symbols could not be loaded for image00400000

image00400000+0x96cf:

004096cf 895c33f8 mov dword ptr [ebx+esi-8],ebx ds:002b:407a1a78=????????
```