Security Advisory 2020-017

Remote-Code-Execution Vulnerabilities in All Versions of Windows

March 27, 2020 — v1.3

TLP:WHITE

History:

- *24/03/2020 — v1.0 – Initial publication*
- *25/03/2020 — v1.1 – Update regarding lack of impact on recent versions of Windows 10*
- *26/03/2020 — v1.2 – Update with info about `fontdrvhost.exe` in Windows 10 build 1709*
- *27/03/2020 — v1.3 – Clarification and reference to 0patch micropatching for Windows 7*

Summary

On the 23th of March 2020, Microsoft released a security advisory for two **remote-code-execution** vulnerabilities **affecting all versions of Windows** [1]. The two vulnerabilities are linked to the **Adobe Type Manager Library**. An attacker could exploit these vulnerabilities by convincing a user to open or preview a specially crafted document.

Microsoft is aware of **ongoing attacks** which could exploit these 0-days vulnerabilities. A patch is not available yet but Microsoft provides advice on workarounds to limit the exploitability of the vulnerabilities.

Update: On the 24th of March 2020, Microsoft updated the advisory, explaining that the attack mostly affect Windows 7 and that **the vulnerability is not considered as critical for recent Windows 10 systems**.

Technical Details

The two 0-day vulnerabilities exist in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font – Adobe Type 1 PostScript format.

Adobe Type Manager (located in `%windir%\system32\atmfd.dll`), is a kernel module that is provided by Windows and provides support for OpenType fonts. This kernel module is loaded when a user opens or previews (*Preview Pane* and *Details Pane* in Windows Explorer) documents containing OpenType fonts.

The change in criticality for Windows 10 build 1709 and later [2] is due to the fact that font parsing was moved to `fontdrvhost.exe`, a sandboxed user-space process. `fontdrvhost.exe` likely shares code with `atmfd.dll`, which explains why those system are also vulnerable [3]. However, the attacker will need another vulnerability to escape the `AppContainer` sandbox. Also note that in some cases, the `atmfd.dll` may still be present on the newer system (build 1709 and later), but will not be used for font parsing.

Apart from exploiting these vulnerabilities by convincing a user to open or preview a specially crafted document, the vulnerability could also be exploited via the `WebClient` service through a remote WebDAV server.

Products Affected

- Windows 10 for 32-bit Systems
- Windows 10 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 Version 1709 for 32-bit Systems
- Windows 10 Version 1709 for ARM64-based Systems
- Windows 10 Version 1709 for x64-based Systems
- Windows 10 Version 1803 for 32-bit Systems
- Windows 10 Version 1803 for ARM64-based Systems
- Windows 10 Version 1803 for x64-based Systems
- Windows 10 Version 1809 for 32-bit Systems
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1903 for 32-bit Systems
- Windows 10 Version 1903 for ARM64-based Systems
- Windows 10 Version 1903 for x64-based Systems
- Windows 10 Version 1909 for 32-bit Systems
- Windows 10 Version 1909 for ARM64-based Systems
- Windows 10 Version 1909 for x64-based Systems
- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows 8.1 for 32-bit systems
- Windows 8.1 for x64-based systems
- Windows RT 8.1
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 for Itanium-Based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Server 2016 (Server Core installation)
- Windows Server 2019
- Windows Server 2019 (Server Core installation)

- Windows Server, version 1803 (Server Core Installation)
- Windows Server, version 1903 (Server Core installation)
- Windows Server, version 1909 (Server Core installation)

Recommendations

Microsoft has not yet released a patch for this vulnerability. It is recommended to apply workarounds until the patch is available.

Workarounds Recommended by Microsoft

Microsoft recommends the following workarounds to limit the scope of the vulnerabilities, especially on versions before Windows 10 build 1709 [1].

Disable the Preview Pane and Details Pane in Windows Explorer

For Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows 8.1, perform the following steps:

- Open Windows Explorer, click *Organize*, and then click *Layout*.
- Clear both the *Details pane* and *Preview pane* menu options.
- Click *Organize*, and then click *Folder and search options*.
- Click the *View* tab.
- Under *Advanced settings*, check the *Always show icons, never thumbnails* box.
- Close all open instances of Windows Explorer for the change to take effect.

For Windows Server 2016, Windows 10, and Windows Server 2019, perform the following steps:

- Open Windows Explorer, click the *View* tab.
- Clear both the *Details pane* and *Preview pane* menu options.
- Click *Options*, and then click *Change folder and search options*.
- Click the *View* tab.
- Under *Advanced settings*, check the *Always show icons, never thumbnails* box.
- Close all open instances of Windows Explorer for the change to take effect.

Disable the `WebClient` Service

Perform the following steps:

- Click *Start*, click *Run* (or press the *Windows Key* and *R* on the keyboard), type `services.msc` and then click *OK*.
- Right-click `WebClient` service and select *Properties*.
- Change the *Startup type* to *Disabled*. If the service is running, click *Stop*.
- Click *OK* and exit the management application.

Rename `atmfd.dll` (only for systems prior to Windows 10 build 1709)

For 32-bit systems, enter the following commands at an administrative command prompt and restart the system:

```
cd "%windir%\system32"
takeown.exe /f atmfd.dll
icacls.exe atmfd.dll /save atmfd.dll.acl
icacls.exe atmfd.dll /grant Administrators:(F)
rename atmfd.dll x-atmfd.dll
```

For 64-bit systems, enter the following commands at an administrative command prompt and restart the system:

```
cd "%windir%\system32"
takeown.exe /f atmfd.dll
icacls.exe atmfd.dll /save atmfd.dll.acl
icacls.exe atmfd.dll /grant Administrators:(F)
rename atmfd.dll x-atmfd.dll
cd "%windir%\syswow64"
takeown.exe /f atmfd.dll
icacls.exe atmfd.dll /save atmfd.dll.acl
icacls.exe atmfd.dll /grant Administrators:(F)
rename atmfd.dll x-atmfd.dll
```

Optional Procedure for Windows 8.1 Operating Systems and Below (Disable `ATMFD`)

Set the following registry key:

```
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\DisableATMFD, DWORD = 1
```

Micropatching

On 26th of March 2020, 0patch proposed a micropatch for Windows 7 64-bit and Windows Server 2008 R2 without Extended Security Updates (ESU) [4].

The patch injects in `gdi32.dll` right before the `syscall` instruction to transfer execution to the kernel in function `NtGdiAddFontResourceW`, successfully covering all common execution points that various Windows applications such as Windows Explorer, Font Viewer, and applications use to parse Adobe Type 1 PostScript fonts.

References

[1] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200006

[2] https://twitter.com/DidierStevens/status/1242387445850791937

[3] https://twitter.com/DidierStevens/status/1242249023303499777

[4] https://blog.0patch.com/2020/03/micropatching-unknown-0days-in-windows.html