American Technology Services
a WWTS Company

2020-02 ATS Security Advisory

Type 1 Font Parsing Remote Code Execution Vulnerability

Summary

On Monday, March 23, 2020, Microsoft's Security Response Center released a Security Advisory documenting vulnerabilities in Adobe Type Manager Library, which is a program built into all currently supported version of Windows. This vulnerability may allow an attacker to craft a document, which, when previewed or opened, can allow remote code execution. As such, this vulnerability has been designated "critical" in severity. Microsoft has observed this vulnerability being used in "limited targeted attacks" against older, unsupported versions of Windows.

A patch for this vulnerability is currently being developed by Microsoft. However, existing mitigations, and additional configuration changes can prevent an attacker from exploiting this vulnerability. **Most importantly, Windows 10 has built-in protections which make negligible the risk of remote code execution by an attacker. The "limited targeted attacks" observed by Microsoft have only affected Windows 7 systems.** For older affected systems, Microsoft has released configuration changes which can mitigate this threat.

What Can You Do?

If you are running an up-to-date version of Windows 10, there is nothing that needs to be done. Mitigations already exist which will prevent an attacker from successfully exploiting this vulnerability. All Windows 10 systems maintained by ATS Managed Services should be protected from this exploit.

Older versions of Windows, including Windows 8, and Windows 7 are vulnerable. **However, known exploitation of this vulnerability is currently observed as "limited targeted attacks" against Windows 7 systems.** Although not stated in the Microsoft Advisory, this follows a pattern of a likely limited attack against a sensitive target carried out by a resourceful adversary, or an Advanced Persistent Threat (APT). It's likely that this will remain true until a public "proof of concept" is released by security researchers. It is likely that a patch will be released before this happens.

2020-02 ATS Security Advisory

Mitigations for these older versions of Windows involve configuration changes to the system, including:

- Disabling the Preview Pane and Details Pane in Windows Explorer
- Disabling the WebClient service
- Rename ATMFD.DLL (on Windows 10 systems that have a file by that name), or alternatively, disable the file from the registry

Specific steps to implement these changes are different in each system. These are documented in Microsoft's Advisory.

Details

Adobe Type Manager (ATM) is a supporting computer program, commonly called a "library" which is used by Windows to process and display PostScript Type I fonts. A vulnerability was discovered which could allow an attacker to gain remote code execution (RCE) on a vulnerable system. Since this vulnerability is being exploited in limited targeted attacks, and no patch has been provided by Microsoft, this vulnerability is known as a "zero-day vulnerability".

To exploit this vulnerability, an attacker would need to create a document containing a crafted, malicious PostScript font. Then, the attacker would need to find a way to force a user, or program, to use the document in such a way that it is processed by ATM. They may send a document via email or upload the document through an online form. Then, if a user opens the document or uses the document "preview" view available in Windows, the attacker could gain remote code execution on that machine.

Windows 10 has a powerful mitigation designed to prevent exactly this kind of "zero-day" vulnerability. A feature called AppContainer isolates the ATM program from the rest of the system. This is known as a "sandboxing" the process. Even if an attacker successfully exploits the underlying vulnerability, AppContainer would prevent an attacker from gaining any visibility or access to the underlying system.

For older systems, including unsupported systems such as Windows 7, Microsoft has provided workarounds that will mitigate the threat altogether. These are configuration changes that

2020-02 ATS Security Advisory

need to be manually applied to affected systems. The full Microsoft Advisory, containing various mitigation steps, is included in the “Notes” section of this document.

Notes

Microsoft Advisory: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv200006