SANDBOX TECHNOLOGIES

Recent Exploit Utilizes Microsoft Office Files to Compromise Computers

Although users should NEVER open unsolicited documents or files of any sort, the recent discovery of a new vulnerability affecting Microsoft Office is a perfect occasion to remind everyone of this important security practice.

While it's widely known that files of uncertain origin shouldn't be opened, the reality is that occasionally people make the mistake of letting their guard down.

New vulnerability

Microsoft recently announced the discovery of what is known as a remote code execution vulnerability. By opening a malicious Microsoft Office file (Word, for example), users can unknowingly open the door for an attacker to install programs, as well as view, alter, exfiltrate or delete data. Although this specific weakness is new, this type of exposure has been in existence for a long time.

What is being done?

Microsoft is currently working on a patch to correct this particular flaw. The target for the release of a patch is currently unknown, but things of this nature are typically addressed quickly.

What can be done in the meantime?

There is a workaround, and it entails disabling what's known as the MDST URL Protocol. This can be accomplished quickly, however current guidance requires that it be done individually on each computer, which unfortunately makes it time consuming in the aggregate when many computers are involved.

As an added drawback to the workaround, disabling the MDST URL Protocol can occasionally impact desired functionality and necessary support services. As such, it is recommended that it be re-enabled after Microsoft has corrected the problem with a patch.

While security best practices recommend implementing the workaround, some organizations have opted to forego it in favor of reminding their users to NEVER open any files of unknown origin.

Ultimately, the decision regarding what approach to take is one that must be made by management. The exposure is very real; however, this particular threat can only be unleashed by opening a maliciously altered MS Office file. For more information, or to request implementation of the temporary workaround protection, simply reply to this email or contact your Sandbox Technologies Engineer or CCIO.

Technical Details

For those interested, technical details pertaining to this threat (commonly referred to as "Follina") can be found on Microsoft's website by visiting the following link:
CVE-2022-30190 - Security Update Guide - Microsoft - Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability

Warm Regards,

Aaron Arlotti
Manager, Remote Support Operations
Sandbox Technologies, Inc.