Microsoft reports new Windows vulnerability

March 24 2020, by Peter Grad

Microsoft reported a "critical" security vulnerability Monday that could affect millions of Windows users. The critical label is the highest severity rating issued to potential threats.

The flaw resides in the Adobe Type Manager Library, which controls how fonts are rendered and displayed.

Hackers can trick users into opening a document containing hidden malicious content. The assault does not require the user to click on a link. Merely viewing the document in a preview screen can trigger the attack.

The vulnerability is found on all recent versions of Windows, including versions 7, 8 and 10, and Windows Server.

At the moment, there is no fix. Until a solution is found, Microsoft recommends three workarounds. They include disabling the Preview and Details panes in Windows explorer, disabling WebClient service and disabling the ATMFD.DLL file in the registry. Alternately, renaming the ATMFD.DLL file will protect the functionality of the program.

But Microsoft cautions that renaming the .DLL file may disrupt functionality of some programs that rely on embedded fonts or OpenType fonts. They also repeated a frequently issued warning that making incorrect changes to Windows registry settings, or making any typos in instructions, exposes users to system crashes that may require a full Windows reinstallation.

Disabling the WebClient service will still leave open the possibility of hackers running programs on the targeted computer or network. But users will be prompted for confirmation before a program is opened, alerting users to suspicious activity.

The Microsoft advisory referred to "limited, targeted attacks," but did not specify who they believe is responsible for this latest assault nor the number or frequency of attacks. Observers note that the phrase "limited, targeted attacks" is shorthand for digital assaults conducted by hackers working on behalf of foreign governments.

The Microsoft advisory posted Monday is titled "Type 1 Font Parsing

Remote Code Execution Vulnerability." Details may be found at https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv200006#march-23-flaw.

The advisory states: "There are multiple ways an attacker could exploit the vulnerability, such as convincing a user to open a specially crafted document or viewing it in the Windows Preview pane."

It continues: "Microsoft is aware of this vulnerability and working on a fix. Updates that address security vulnerabilities in Microsoft software are typically released on Update Tuesday, the second Tuesday of each month. This predictable schedule allows for partner quality assurance and IT planning, which helps maintain the Windows ecosystem as a reliable, secure choice for our customers."

More information: portal.msrc.microsoft.com/en-u … 200006#march-23-flaw

Citation: Microsoft reports new Windows vulnerability (2020, March 24) retrieved 9 April 2024 from https://techxplore.com/news/2020-03-microsoft-windows-vulnerability.html