Microsoft admits a new zero-day vulnerability threatens millions of Windows users

According to Microsoft, this new zero-day vulnerability affects all versions of Windows from Windows 7 to Windows 10 and corresponding versions of Windows Server.

Microsoft has just acknowledged a Windows zero-day vulnerability in MSHTML that allows hackers to execute code remotely if exploited successfully. This vulnerability affects all versions of Windows from Windows 7 to Windows 10 and corresponding versions of Windows Server.

Currently, Microsoft is tracking the vulnerability under the codename CVE-2021-40444 and further claims that hackers will exploit the vulnerability by distributing malicious Office documents. According to the CVE scale, the new vulnerability has a severity level of 8.8.

In more detail, Microsoft says hackers can create an ActiveX control using Office's MSHTML browser rendering engine. When the user opens it, it triggers a remote code execution attack.

However, users who use the default option to open files from the internet via Protected View or via Application Guard for Office will not be attacked. Furthermore, according to Microsoft, Defender Antivirus and Defender for Endpoint can also successfully detect threats.

Another solution that Microsoft offers is to turn off all settings related to ActiveX controls through the Registry Editor. This change does not affect installed controls.

Here's how to disable an ActiveX control:

1. Open Notepad
2. Copy the following lines and paste in Notepad

```
Windows Registry Editor Version 5.00 [HKEY_LOCAL_MACHINESOFTWAREPoliciesMicrosof
```

1. Save the Notepad file as a .reg . file
2. Double click on the saved file to apply the changes to the Registry
3. Restart the machine

> **Note:** If you do the above operations, 3 new keys will be created in Registry Editor. To re-open the ActiveX control you will have to find and delete the keys you just created.

Microsoft is currently investigating and will take appropriate action when it completes its assessment of this vulnerability. Most likely in the near future Microsoft will release a patch or permanent damage reduction for it.