Issued 6/15/17

All Windows Users, Update Your Systems ASAP

Microsoft rolled out this month's Patch Tuesday updates a few hours ago, and the company confirmed that it's already aware of attacks trying to exploit some of the known vulnerabilities, urging users to patch their systems as soon as possible. First of all, there's vulnerability CVE-2017-8543 and which is affecting absolutely all Windows versions out there, including those that are no longer getting support from Microsoft. This is a Remote Code Execution flaw in the Windows Search service which allows an attacker to take control of a vulnerable system. The update is released for all Windows versions from Windows XP to Windows 10, even though the older releases are no longer getting support. Microsoft says that its decision to patch unsupported versions of Windows is based on evidence pointing to possible attacks launched by government organizations, so in order to protect users, the company published a Windows XP, Windows Vista, and Windows Server 2003 patch as well. "To exploit the vulnerability, the attacker could send specially crafted SMB messages to the Windows Search service. An attacker with access to a target computer could exploit this vulnerability to elevate privileges and take control of the computer. Additionally, in an enterprise scenario, a remote unauthenticated attacker could remotely trigger the vulnerability through an SMB connection and then take control of a target computer," Microsoft says.

The second vulnerability that's currently under attack is CVE-2017-8464 and it targets the way an icon is displayed if malicious code is injected. "The attacker could present to the user a removable drive that contains a malicious shortcut file and an associated malicious binary. When the user opens this drive in Windows Explorer, or any other application that parses the icon of the shortcut, the malicious binary will execute code of the attacker's choice on the target system," Microsoft explains. While these vulnerabilities are already being exploited by attackers across the world, Microsoft Edge and Internet Explorer flaws documented as CVE-2017-8498, CVE-2017-8530 and CVE-2017-8523 have already been disclosed, but without any attacks detected so far. But given that all details are already public, it's just a matter of time until cybercriminals include them in their exploit kits.