Issued 8/10/17

'Critical' Windows Bug Squashed by Microsoft in Patch Tuesday Update

Microsoft has patched a flaw that left every modern version of Windows vulnerable to malware that could take over a PC and spread between machines. The vulnerability in the code for Windows Search was described by researchers at security firm Trend Micro as "by far the most critical bug" fixed as part of August's Patch Tuesday update. This flaw, which Microsoft has warned is likely to be exploited, could allow an attacker to take full control of a system, with the ability to install and run programs, and to delete data. But what makes this vulnerability particularly dangerous, according to Trend Micro, is that it can be exploited remotely by an unauthenticated machine over the Server Message Block (SMB) networking protocol.

The rapid spread of WannaCry and Petya during the recent global outbreaks was, in part, due to the malware using the EternalBlue exploit for an SMB vulnerability to spread between machines. The Windows Search flaw can be exploited by attackers sending a specially crafted message to the service, and system administrators who can't update Windows systems are recommended to disable WSearch using the instructions outlined here. Altogether, 48 security holes were fixed by Microsoft in this latest update, with 25 of the vulnerabilities rated as critical security risks. Other notable fixes include the first patch for a flaw in Windows Subsystem for Linux, the code that allows Windows 10 to run Linux command line tools inside Windows Store apps. By

exploiting the fact the system can handle certain objects improperly in memory, the attacker could trigger a denial of service attack against the system. The attack requires the user to run a specially crafted application and is deemed by Microsoft to be unlikely to be exploited.

Other software patched in this update include Internet Explorer, Adobe's Flash Player, SharePoint, SQL Server and the Hyper-V hypervisor, which has a vulnerability that could allow allow applications running in a guest OS in a VM to run code on the host machine.