Issued 5/11/17

Microsoft Scrambles to Fix Worst Windows Issue 'in Recent Memory'

Called the “worst Windows remote code exec in recent memory” and "crazy bad" by the Google security expert that discovered it, the malware requires no interaction from a user. Often malware requires a PC user to, for example, click on a bad link or do something that -- unbeknownst to the user -- downloads rogue code. The fact that Microsoft took action immediately to fix it – a so-called “emergency out- of-band update” – means it’s very serious. “Unlike past incidents, where Microsoft has allowed exploited zero- day vulnerabilities to fester in the wild without being bothered to deliver a patch for months, this time around, the company moved lightning fast to address the issue,” according to a report at Bleeping Computer.

Zero-day vulnerabilities are defined as a vulnerability not made public before becoming active, meaning that the entity responsible for the software with the vulnerability has, in effect, zero days to fix the problem. The Microsoft fix was issued on Monday. “Customers are protected by an update released on Monday, May 8. More information is available in our security advisory," a Microsoft spokesperson told Fox News. What makes this exploit worrisome on a broader level is the very nature anti-malware software. "That's one of the big problems with anti-malware software: by trying to protect the system from every angle, they also expose their own vast attack surface," said Ars Technica. The vulnerability was discovered last week by Tavis Ormandy and Natalie Silvanovich. Ormandy is a vulnerability researcher at Google, while Silvanovich also works at Google. Ormandy said in a tweet that the exploits were "wormable," meaning they could self-replicate and move to other vulnerable computers.

The security hole affects PCs and computer systems running Windows 7, Windows 8.1, Windows 10, and Windows Server 2016 and Microsoft software products running on those systems and exploits the Microsoft Malware Protection Engine included on Windows 7 and later. The vulnerability can be triggered “if the Microsoft Malware Protection Engine scans a specially crafted file,” according to the Microsoft Security Advisory.

That could include email and web sites. That is, anything this is scanned by the Malware Protection Engine. That engine is part of Microsoft’s Windows Defender which is preinstalled on PCs. The Microsoft advisory goes on to say that IT administrators and individual users should not need to proactively install the update. “Typically, no action is required of enterprise administrators or end users to install updates for the Microsoft Malware Protection Engine, because the built-in mechanism for the automatic detection and deployment of updates will apply the update within 48 hours of release.”