SSBG IT Solutions

Ph: (8621) 5404-3999 Fax: (8621) 5404-7759
Email: Sales1@SSBG.com.cn www.SSBG.com.cn

A VICIOUS MICROSOFT BUG LEFT A BILLION PCS EXPOSED

MICROSOFT'S SECURITY TEAM had a busy weekend.
On Friday night, security researcher Tavis Ormandy of Google's Project Zero announced on Twitter that he had found a Windows bug. Well, not just any bug. It was "crazy bad," Ormandy wrote. "The worst Windows remote code exec in recent memory." By Monday night, Microsoft had released an emergency patch, along with details of what the vulnerability entailed. And yes, it was every bit as scary as advertised.
That's not only because of the extent of the damage hackers could have done, or the range of devices the bug affected. It's because the bug's fundamental nature underscores the vulnerabilities inherent in the very features meant to keep our devices safe.

Bad Bug

What made this particular bug so insidious was that it would have allowed hackers to target Windows Defender, an antivirus system that Microsoft builds directly into its operating system. That means two things: First, that it impacted the billion-plus devices that have Windows Defender installed. (Specifically, it took advantage of the Microsoft Malware Protection Engine that underpins several of the company's software security products.) Second, that it leveraged that program's expansive permissions to enable general havoc, without physical access to the device or the user taking any action at all.

"This was, in fact, crazy bad," says Core Security systems engineer Bobby Kuzma, echoing Ormandy's original assessment.

As Google engineers note in a report on the bug, to pull off the attack a hacker would have only had to send a specialized email or trick a user into visiting a malicious website, or otherwise sneak an illicit file onto a device. This also isn't just a case of clicking the wrong link; because Microsoft's antivirus protection automatically inspects every incoming file, including unopened email attachments, all it takes to fall victim is an inbox.

"The moment [the file] hits the system, the Microsoft malware protection intercepts it and scans it to make sure it's 'safe,'" says Kuzma. That scan triggers the exploit, which in turn enables remote code execution that enables a total machine takeover. "As soon as it's there, the malware protection will take it up and give it root access."

It's scary stuff, though tempered by Microsoft's quick action and the fact that Ormandy appears to have found the bug before bad actors did. And because Microsoft issues automatic updates for its malware protection, most users should be fully protected soon, if not already. It should still serve as an object lesson, though, in the risks that come with antivirus software that has tendrils in every part of your system.

Security Trade-Offs

It’s a scary world out there, and antivirus generally helps make it less so. To do its job correctly, though, it needs unprecedented access to your computer—meaning that if it falters, it can take your entire system down with it.

“There is a raging debate about antivirus in some circles, stating that it can be used as a springboard to infect users,” says Jérôme Segura, lead malware intelligence analyst with Malwarebytes. “The fact of the matter is that security software is not immune to flaws, just like any other program, but there is no denying the irony when an antivirus could be leveraged to infect users instead of protecting them.”

Irony and, well, damage. A year ago, Google’s Ormandy found critical vulnerabilities that affected no fewer than 17 Symantec antivirus products. He’s found similar in offerings from security vendors like FireEye, McAfee, and more. And more recently, researchers discovered an attack called “DoubleAgent,” which turned Microsoft’s Application Verifier tool into a malware entry point.

“Because of what they do, AV products are really complex and have to touch a lot of things that are untrusted,” says Kuzma. “This is the kind of vulnerability we’ve seen time and again.”

There’s also no real solution; it’s not easy to weigh the protections versus the risks. The best you can hope for, really, is what Ormandy and Microsoft demonstrated during the last few days: That someone catches the mistakes before the bad guys do, and that the fixes come fast and easy.

Link: https://www.wired.com/2017/05/vicious-microsoft-bug-left-billion-pcs-exposed/
AUTHOR: BRIAN BARRETT