

BRIAN BARRETT SECURITY MAY 15, 2019 12:28 PM

Microsoft's First Windows XP Patch in Years Is a Very Bad Sign

A very bad vulnerability in Windows XP could have serious ramifications, even with a patch.



LA TIGRE



THIS WEEK, MICROSOFT issued patches for 79 flaws across its platforms and

products. One of them merits particular attention: a bug so bad that [Microsoft released a fix for it on Windows XP](#), an operating system it officially abandoned five years ago.

There's maybe no better sign of a vulnerability's severity; the last time Microsoft bothered to make a Windows XP fix publicly available was a little over two years ago, in the months before the [WannaCry ransomware attack swept the globe](#). This week's vulnerability has similarly devastating implications. In fact, Microsoft itself has drawn a direct parallel.

Daily Newsletter

Our biggest stories, handpicked for you each day.

SIGN UP

By signing up, you agree to our [user agreement](#) (including [class action waiver and arbitration provisions](#)), and acknowledge our [privacy policy](#).

“Any future malware that exploits this vulnerability could propagate from vulnerable computer to vulnerable computer in a similar way as the WannaCry malware spread across the globe in 2017,” Simon Pope, director of incident response for the Microsoft Security Response Center, [wrote](#) in a statement announcing the patch Tuesday. “It is highly likely that malicious actors will write an exploit for this vulnerability and incorporate it into their malware.”

Microsoft is understandably withholding specifics about the bug, noting only that it hadn't seen an attack in action yet, and that the flaw relates to Remote Desktop Services, a feature that lets administrators take control of another computer that's on the same network.

That small parcel of information, though, still gives potential attackers plenty enough to go on. “Even mention that the area of interest is Remote Desktop

Protocol is sufficient to uncover the vulnerability,” says Jean Taggart, senior security researcher at security firm Malwarebytes.

Expect that to happen quickly. “This will be fully automated in the next 24 to 48 hours and exploited by a worm,” says Pieter Danhieux, CEO of secure coding platform Secure Code Warrior, referring to the class of malware that can propagate across a network without any human interaction, such as clicking the wrong link or opening the wrong attachment. Like the Blob, it just spreads.

Once that worm gives hackers access to those devices, the possibilities are fairly limitless. Danhieux sees ransomware as a likely path; Taggart ticks off spam campaigns, DDoS, and data harvesting as possibilities. “Take your pick,” he adds. “Suffice to say, a lot.”

The saving grace for all of this is that computers running Windows 8 and up aren’t affected. But it’s important not to underestimate the danger that Windows XP computers can still pose. Estimates vary, but analytics company Net Marketshare says that 3.57 percent of all desktops and laptops still run Windows XP, which was first released in 2001. Conservatively, that’s still tens of millions of devices on Windows XP—more than are running on the most recent version of MacOS. Moreover, you can assume with some confidence that almost none of those computers are ready for what’s coming.

"When you're dealing with patching, it's a balancing act."

— RICHARD FORD, FORCEPOINT

Yes, plenty of Windows XP users are just folks who haven’t dusted off their Dell Dimension tower since the last Bush administration. It seems unlikely that they’ll ever get around to installing this latest patch, especially given that you need to seek it out, and download and install it yourself. It’s hard enough to get people to update modern systems with their incessant nagging popups; one imagines that those still on Windows XP are in no rush to visit the Microsoft Update Catalog.

More troubling, though, are the countless businesses and infrastructure concerns

that still rely on Windows XP. As recently as 2016, even nuclear submarines had it on board. For the most sensitive use cases—like, say, nukes—companies and governments pay Microsoft for continued security support. But the bulk of hospitals, businesses, and industrial plants that have Windows XP in their systems don't. And for many of those, upgrading—or even installing a patch—is more difficult than it might seem.

“Patching computers in industrial control networks is challenging because they often operate 24/7, controlling large-scale physical processes like oil refining and electricity generation,” says Phil Neray, vice president of industrial cybersecurity at CyberX, an IoT and ICS-focused security firm. Recent CyberX research indicates that more than half of industrial sites run unsupported Windows machines, making them potentially vulnerable. There's not much opportunity to test the impact of a patch on those types of systems, much less to interrupt operations to install them.



That applies to health care systems, too, where the process of updating critical software could interrupt patient care. Other businesses run specialized software that's incompatible with more recent Windows releases; practically speaking, they're trapped on XP. And while the best way to protect yourself from this latest vulnerability—and the countless others that now plague unsupported operating systems—is to upgrade to the latest version of Windows, cash-strapped businesses tend to prioritize other needs.

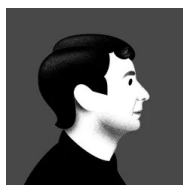
With any luck, Microsoft's extraordinary step of pushing a patch will spur many of them to action. It's hard to imagine a louder siren. “When you're dealing with patching, it's a balancing act between the costs of patching and the costs of leaving it alone, or just asking users to upgrade,” says Richard Ford, chief scientist at cybersecurity firm Forcepoint. “They would have a grasp of both the security risk—and the reputational risk—of not going after this vulnerability aggressively. Put those all together, and when the stars align it makes a lot of sense to provide the patch, quickly, safely, and even for operating systems that are out of support.”

The coming weeks and months should show, though, just how wide a gap exists between providing a patch and getting people to install it. An attack on Windows

XP is at this point inevitable. And the fallout might be worse than you'd have guessed.

More Great WIRED Stories

- The hacker group on a [supply-chain hijacking spree](#)
- My search for a boyhood friend [led to a dark discovery](#)
- LA's plan to reboot its bus system [using cell phone data](#)
- The antibiotics business is broken, [but there's a fix](#)
- Move over, San Andreas: There's a [new fault in town](#)
-  Upgrade your work game with our Gear team's [favorite laptops, keyboards, typing alternatives, and noise-canceling headphones](#)
-  Want more? [Sign up for our daily newsletter](#) and never miss our latest and greatest stories



[Brian Barrett](#) is the executive editor of news at WIRED, overseeing day to day coverage across the site. Prior to WIRED he was the editor in chief of the tech and culture site Gizmodo and was a business reporter for the Yomiuri Shimbun, Japan's largest daily newspaper.

EXECUTIVE EDITOR, NEWS 

TOPICS [WANNACRY](#) [MICROSOFT](#) [RANSOMWARE](#)

The Daily newsletter

Our biggest stories, handpicked for you each day.

SIGN UP

By signing up, you agree to our [user agreement](#) (including [class action waiver and arbitration provisions](#)), and acknowledge our [privacy policy](#).

READ MORE

The War on Passwords Is One Step Closer to Being Over

“Passkeys,” the secure authentication mechanism built to replace passwords, are getting more portable and easier for organizations to implement thanks to new initiatives the FIDO Alliance announced on Monday.

LILY HAY NEWMAN

Shopping for a Router Sucks. Here's What You Need to Know

How much speed do you need? And what's a MU-MIMO? We decipher the jargon and explain what to look for.

SIMON HILL

Zero-Click Flaw Exposes Potentially Millions of Popular Storage Devices to Attack

A vulnerability categorized as "critical" in a photo app installed by default on Synology network-attached storage devices could give attackers the ability to steal data and worse.

KIM ZETTER

Inside a Firewall Vendor's 5-Year War With the Chinese Hackers Hijacking Its Devices

Sophos went so far as to plant surveillance “implants” on its own devices to catch the hackers at work—and in doing so, revealed a glimpse into China's R&D pipeline of intrusion techniques.

ANDY GREENBERG

‘We’re a Fortress Now’: The Militarization of US Elections Is Here

From bulletproof glass, drones, and snipers to boulders blocking election offices, the US democratic system is bracing for violent attacks in 2024.

DAVID GILBERT

12 Ways to Upgrade Your Wi-Fi and Make Your Internet Faster

From changing Wi-Fi channels to routing an Ethernet cable, there's always something you can do to improve your internet at home.

SCOTT GILBERTSON

Cybercriminals Pose a Greater Threat of Disruptive US Election Hacks Than Russia or China

A report distributed by the US Department of Homeland Security warned that financially motivated cybercriminals are more likely to attack US election infrastructure than state-backed hackers.

LILY HAY NEWMAN

Man Arrested for Snowflake Hacking Spree Faces US Extradition

Alexander “Connor” Moucka was arrested this week by Canadian authorities for allegedly carrying out a series of hacks that targeted Snowflake’s cloud customers. His next stop may be a US jail.

MATT BURGESS

NordVPN Coupon: Up to 74% Off + 3 Months Free

Save 74% and get 3 months free when you sign up for a 2-year plan with this NordVPN discount code.

SCOTT GILBERTSON

All the Top New Features in macOS Sequoia

Apple Intelligence for the Mac is here via macOS 15.1. Here's how to install it, get new features, and figure out whether your current Mac will support the latest capabilities.

BRENDA STOLYAR

A Mysterious Hacking Group Has 2 New Tools to Steal Data From Air-Gapped Machines

It's hard enough creating one air-gap-jumping tool. Researchers say the group GoldenJackal did it twice in five years.


DAN GOODIN, ARS TECHNICA

This AI Tool Helped Convict People of Murder. Then Someone Took a Closer Look

Global Intelligence claims its Cybercheck technology can help cops find key evidence to nail a case. But a WIRED investigation reveals the smoking gun often appears far less solid.

TODD FEATHERS



 YOUR PRIVACY CHOICES