Microsoft alerts hospitals to fix potential security risk

May 16 2019, by Joe Carlson, Star Tribune (Minneapolis)

Credit: CC0 Public Domain

Computer experts inside hospitals were working diligently on Wednesday to address a serious new security vulnerability in older versions of the Windows operating system, which is still used in many

health care devices even though Microsoft hasn't actively supported the older software in years.

Julie Flaschenriem, chief information officer at Hennepin Healthcare, said the Minneapolis health system activated a command center Tuesday evening when news of the vulnerability broke. As of Wednesday, the team was working through its prioritized list of action items for securing any older devices that need attention.

"We know—and the whole world knows—that there are people out there that are trying to exploit this one. And every organization around here, whether it's health care or any other thing, is trying to prevent it," said Flaschenriem, who has held information-technology roles at several health systems in the Twin Cities. "We all have certain risks around this that we work to mitigate. ... Because this has happened enough now, we have plans in place that we can put together and start working on it the minute something like this happens."

On Tuesday, Microsoft began urging users of older operating systems to immediately install security patches or take other steps to secure themselves from a vulnerability that could be exploited and quickly spread global chaos, as happened in 2017 with the so-called "WannaCry" ransomware attack.

In that case, the attack proved destructive even though the security patch to fix it had been available for months. WannaCry affected thousands of unpatched computers worldwide, bringing down hospital networks in the United Kingdom and causing the cancellation of 19,000 medical appointments there two years ago.

"Now that I have your attention, it is important that affected systems are patched as quickly as possible to prevent such a scenario from happening," Simon Pope, director of incident response at the Microsoft

Security Response Center, wrote in a blog post Tuesday. "We are taking the unusual step of providing a security update for all customers to protect Windows platforms, including some out-of-support versions of Windows."

On Tuesday, Microsoft revealed a "zero day" vulnerability in older operating systems that have a feature called "remote desktop protocol." RDP is the system that lets a user remotely control a computer, like when a company's help desk personnel take control of a computer remotely while troubleshooting a problem.

The vulnerability is considered "highly likely" to be incorporated into malware in the near future, judging by Microsoft's proprietary risk score and the CVSS base risk score of 9.8. (CVSS is a 1-10 scale, with higher numbers representing more severe security risks.)

The vulnerability, which has not yet been exploited by malicious hackers, requires no user interaction and can spread easily among unpatched computers on a network, similar to the WannaCry malware.

"The thing that makes this one so dangerous is that you don't need any access," said Jeremy Sneeden, a manager in the threat and vulnerability management department at Allina Health, which owns and operates 13 hospitals in Minnesota and Wisconsin. "A lot of vulnerabilities you need a username and password, or some sort of access to the machine, to make the vulnerability work. But these—I guess they're calling them 'wormable' now—they don't need credentials, and that's why they spread so quickly."

Sneeden said Allina was handling vulnerability countermeasures Wednesday as part of its normal computer-security work, which involves constantly looking for vulnerabilities and prioritizing those that need addressing first. Although Allina has more than 35,000 workstations and

desktop computers, most of them are already running on newer versions of Windows that are not affected.

The cybersecurity vulnerability (which goes by the technical name CVE-2019-0708) affects older operating systems that Microsoft still actively supports—including Windows 7, Windows Server 2008 R2, and Windows Server 2008—as well as systems that are no longer actively supported, including Windows 2003 and Windows XP.

Microsoft says the patch will automatically be installed on supported machines, if the user or network administrator has enabled automatic updates. The updates for unsupported machines are available from Microsoft Windows Security support—just as the patches for the WannaCry vulnerability were available before the large-scale attack.

"WannaCry was a wake-up call for everyone in health care; everyone I talk to puts it that way," said med-tech cybersecurity expert Ben Ransford, the Seattle-based CEO of Virta Labs. "But it's been two years and many health care organizations are still wringing their hands trying to figure out what they should do about unpatched equipment. They've had ample time to get their houses in order after close calls with WannaCry, and most haven't, despite the best efforts of their overtaxed workers, even at top hospitals."

The vulnerability is not specifically targeted at health care organizations like hospitals.

However, hospitals may use older software systems because it can be expensive and time-consuming to do updates on machines that are mobile and widely distributed across a hospital campus. Also, updating software can cause unintended conflicts and glitches elsewhere in a hospital's interconnected IT infrastructure, which can be risky because so many critical machines run on a hospital network.

Information technology staff with Hennepin Healthcare and Allina have both taken special measures previously to protect vulnerable biomedical and diagnostic machines by isolating them in computer networks so that they can only communicate with the minimum number of systems to work correctly, among other precautions.

Software in long-lasting health care machines and implantable devices is often older than what consumers are used to because it takes so long to get new medical devices approved and installed in a hospital. For example, it can take years to get a new MRI scanner onto the market and into the hospital, which means that by the time the system is ready to be installed, the underlying Microsoft operating system may already be old.

"I think every health care organization has that problem," Sneeden said. "The real problem is it takes the medical device manufacturers so long to get the devices approved, that by the time they get approved and purchased and put in, often the operating systems are ancient. And the new ones aren't approved. So we literally cannot do anything about this."