Report on Patient Privacy Volume 20, Number 9. September 10, 2020 Nonpandemic Security Risks Need Attention Now, Warn FBI, Experts

By Jane Anderson

When the COVID-19 pandemic took hold in March, those charged with information technology (IT) security at health care organizations moved quickly to shore up defenses on the particular issues brought to the forefront by the crisis, including those surrounding the increase of telehealth and telework.

But as the crisis moves well past the six-month mark and health care entities settle into what has become a new normal, the FBI and others are warning that certain security risks unrelated to the pandemic may be overlooked, potentially leading to breaches.

Windows 7 end-of-life issues continue to be one of the top unaddressed security issues for health care organizations. However, ransomware and risks associated with remote electronic medical record (EMR) access also are coming to the forefront.

Windows 7 May Be ‘Vulnerable to Exploitation’

Microsoft Corp. ended support for the popular and ubiquitous Windows 7 operating system in January 2020, unless certain customers purchased an Extended Security Update (ESU) plan, which is paid, per-device plan available for Windows 7 Professional and Enterprise versions, with a price that increases the longer a customer continues use. Microsoft will offer the ESU plan until January 2023.[1]

For those Windows 7 customers that opted against purchasing the ESU plan, the FBI is warning that it has observed cybercriminals targeting computer network infrastructure after those networks’ operating systems achieve end-of-life status and the manufacturer stops support.

“Continuing to use Windows 7 within an enterprise may provide cyber criminals access into computer systems,” the FBI said in a statement.[2] “As time passes, Windows 7 becomes more vulnerable to exploitation due to lack of security updates and new vulnerabilities discovered. Microsoft and other industry professionals strongly recommend upgrading computer systems to an actively supported operating system.”

This potentially is a major problem, since Windows 7 may be the most-used operating system in health care, the FBI said. According to the FBI, one report from May 2019 indicated that 71% of Windows devices used in health care ran an operating system that became unsupported in January 2020.

“Increased compromises have been observed in the healthcare industry when an operating system has achieved end of life status,” the FBI said. “After the Windows XP end of life on 28 April 2014, the healthcare industry saw a large increase of exposed records the following year.”

Cybercriminals continue to find entry points into legacy Windows operating systems and leverage Remote Desktop Protocol (RDP) exploits, the FBI said. For example, “Microsoft released an emergency patch for its older operating systems, including Windows 7, after an information security researcher discovered the RDP vulnerability called BlueKeep in May 2019.”

“Since the end of July 2019, malicious RDP activity has increased with the development of a working commercial exploit for the BlueKeep vulnerability,” the FBI said. “Cyber criminals often use misconfigured or improperly secured RDP access controls to conduct cyber attacks. The xDedic Marketplace, taken down by law enforcement in 2019, flourished by compromising RDP vulnerabilities around the world.”

In 2017, roughly 98% of systems infected with the infamous WannaCry ransomware employed Windows 7-based operating systems, the FBI said. After Microsoft released a patch in March 2017 for the computer exploit that WannaCry exploited, many Windows 7 systems remained unpatched when the attacks began in May 2017.

“With fewer customers able to maintain a patched Windows 7 system after its end of life, cyber criminals will continue to view Windows 7 as a soft target,” the FBI said.