Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

3 August 2020

PIN Number
20200803-002

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This product was coordinated with DHS-CISA.

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Computer Network Infrastructure Vulnerable to Windows 7 End of Life Status, Increasing Potential for Cyber Attacks

Summary

The FBI has observed cyber criminals targeting computer network infrastructure after an operating system achieves end of life status. Continuing to use Windows 7 within an enterprise may provide cyber criminals access into computer systems. 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.

Migrating to a new operating system can pose its own unique challenges, such as cost for new hardware and software and updating existing custom software. However, these challenges do not outweigh the loss of intellectual property and threats to an organization.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat Overview

On 14 January 2020, Microsoft ended support for the Windows 7 operating system, which includes security updates and technical support unless certain customers purchased an Extended Security Update (ESU) plan. The ESU plan is paid per-device and available for Windows 7 Professional and Enterprise versions, with an increasing price the longer a customer continues use. Microsoft will only offer the ESU plan until January 2023. Continued use of Windows 7 creates the risk of cyber criminal exploitation of a computer system.

- As of May 2019, an open source report indicated 71 percent of Windows devices used in healthcare organizations 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. After the Windows XP end of life on 28 April 2014, the healthcare industry saw a large increase of exposed records the following year.

- Cyber criminals continue to find entry points into legacy Windows operating systems and leverage Remote Desktop Protocol (RDP) exploits. 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. 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 percent of systems infected with WannaCry employed Windows 7 based operating systems. After Microsoft released a patch in March 2017 for the computer exploit used by the WannaCry ransomware, many Windows 7 systems remained unpatched when the WannaCry 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.

Recommendations

Defending against cyber criminals requires a multilayered approach, including validation of current software employed on the computer network and validation of access controls and network configurations. Consideration should be given to:

- Upgrading operating systems to the latest supported version.
- Ensuring anti-virus, spam filters, and firewalls are up to date, properly configured, and secure.
- Auditing network configurations and isolate computer systems that cannot be updated.
- Auditing your network for systems using RDP, closing unused RDP ports, applying two-factor authentication wherever possible, and logging RDP login attempts.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey