Serianu Cyber Security Advisory

Computer Network Infrastructure Vulnerable to Windows 7

Serianu SOC Advisory Number:

TA – 2020/009

Date(s) issued:

14th August 2020

Systems Affected

- Windows 7 Operating System

OVERVIEW

Serianu research team has observed cyber criminals targeting computer network infrastructure after an operating system achieves end of life status. According to our research, organizations continuing to operate with Microsoft Windows 7 platforms on the network infrastructure are at an increased risk of cyberattacks. Windows 7 continues to become more vulnerable to exploitation due to lack of security updates and new vulnerabilities discovered.

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.

This advisory is issued to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

Threat Overview

On 14th January 2020, Microsoft ended support for windows 7 operating system which includes security updates and technical support unless customers purchased an extended security update (ESU) plan. The ESU plan is paid per-device and available for windows 7 professional and enterprise version, with an

increase price the longer a customer continues to use. Microsoft will only offer ESU plan until January 2023. Continuous use of Windows 7, creates the risk of cybercriminal exploitation of computer system.

As of May 2019, 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 28th April 2014, the healthcare industry saw a large increase of exposed records the following year.

Furthermore, cyber criminals continue to find entry points into legacy windows operating systems and leverage exploits on the Remote Desktop Protocol (RDP). Microsoft released an emergency patch for its older operating systems including windows 7, after the RDP vulnerability called BlueKeep was discovered in May 2019.The CVE-2019-0708 vulnerability, referred to as BlueKeep in the RDP or terminal services, would give a hacker remote access to systems without authorization and allow an attacker to send requests through the RDP including a malware infection able to infect all connected devices.

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 WannaCry ransomware, many windows 7 systems remained unpatched when WannaCry ransomware began in May 2017. With fewer organisations able to maintain a patched windows 7 systems 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, access controls and network configurations. Serianu recommends the following as mitigation procedures:

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

Information Sharing

As a means of preventing such attacks from occurring, we encourage any organisation or individual that has access to information concerning malicious related activities from cyber attackers to share it with us through our email: info@serianu.com.