Homeland Security warns of Windows worm

June 9 2020, by Peter Grad

Credit: Pixabay/CC0 Public Domain

The Homeland Security's cybersecurity advisory division is cautioning Windows 10 users of the possibility of a wave of cyberattacks due to the recent publication of an exploit code.

"Malicious cyber actors are targeting unpatched systems with the new [threat]," the agency noted on the Homeland Security web site. The

agency said it "strongly recommends using a firewall to block server message block ports from the internet and to apply patches to critical- and high-severity vulnerabilities as soon as possible."

The agency also referred concerned parties to Microsoft's security guidance posts and notes published by the U.S. Computer Emergency Readiness Team at us-cert.gov.

A Github user published the proof-of-concept exploit code Monday. On unpatched systems, the code potentially could spread to millions of computers. In the hands of malicious actors, the losses could be massive, with estimates ranging from billions to tens of billions of dollars.

The user noted that the exploit itself contains flaws, stating, "It was written quickly and needs some work to be more reliable." The user noted that the code frequently crashes a system, resulting in a BSOD—blue screen of death.

The exploit, termed SMBGhost, is not easy for hackers to successfully execute. But security officials warn the wormlike nature of the exploit, paired with tendency of computer users to delay patching systems with the latest updates, is reason for concern.

The Windows flaw is located in the Server Message Block (SMB), where files, printers and other accessories linked through local networks or the Internet communicate with one another.

A malicious packet can enter the system and, without any user activity, spread to millions of other users.

This latest vulnerability recalls two devastating cyberattacks, both implemented via worms, that occurred a few years ago.

In 2017, a ransomware worm called WannaCry encrypted data on more than 200,000 computers in 150 countries and issued demands ransom using Bitcoin cryptocurrency. An emergency patch was distributed within days and a kill switch implemented that halted the worm's spread. But experts say damages may have reached as high as billions of dollars. The attack was believed to have been launched from North Korea.

Similarly, NotPetya the same year infected an accounting program widely used in Ukraine and reached businesses around the globe. Although it, too, caused billions of dollars in damage, it was not believed to be primarily designed to make money. A security report examining the attack said it did not appear to be designed for "coercion or conquest." A University of California Berkley computer scientist called the attack "a deliberate, malicious, destructive attack or perhaps a test disguised as ransomware."

Microsoft urged all users of Windows 10 versions 1903 and 1909 and Windows Server versions 1903 and 1909 to instal patches.

"We recommend customers install updates as soon as possible as publicly disclosed vulnerabilities have the potential to be leveraged by bad actors," Microsoft cautioned in a statement Friday. "An update for this vulnerability was released in March, and customers who have installed the updates, or have automatic updates enabled, are already protected."

Microsoft also noted that workarounds such as disabling SMB compression and blocking port 445 may fend off attacks but that neither one corrects the underlying vulnerability.

More information: www.us-cert.gov/ncas/current-a … erable-cve-2020-0796