Millions of old phones, laptops, and smart gadgets could stop working later this week for a weird reason

The internet connectivity on older tech devices and smart gadgets could stop working on Thursday after a key digital certificate required to access websites safely expires.© Provided by Washington Examiner.

Let's Encrypt, a nonprofit organization that is the largest issuer of digital certificates — which encrypts and protects the connection between devices and websites on the internet — will be forced to expire one of its most popular digital certificates, the IdentTrust DST Root CA X3, on Sept. 30.

This means several phones, computers, video game consoles, smart gadgets, and "Internet of Things" devices bought before 2017 that use the Let's Encrypt digital certificate in question, and haven't updated their software since then, could face significant issues connecting to the internet.

The problem will primarily affect popular devices, such as iPhones running iOS 9 and below, Android phones running below the 2.3.6 software, Windows computers running software prior to XP SP3, Sony's PS3, and PS4 game consoles, and the Nintendo 3DS.

“Certain older devices from 2016 and before and any gadget that has the word ‘smart’ in it that requires internet connectivity, like certain TVs, bulbs, fridges, and home control apps, could be affected by this certificate expiry,” said security researcher and cybersecurity expert Scott Helme. “It's not clear how big of a problem this will be, but something somewhere will certainly break. There will be a bunch of fires tomorrow, and we'll just have to put them out."

This problem has flown under the radar of many manufacturers, including Big Tech companies Apple, Google, Sony, and Microsoft — none of which have made announcements to customers about potential issues, Helme said.

He added this is one of the first major digital certificates to expire since the advent of the internet in the 1980s. Therefore, there is no precedent for how to solve the problem besides updating the software on devices.

“There have been no squeaky wheels, so no one has ever oiled it. It’s a brand-new problem,” Helme said.

Planned obsolescence, which makes tech devices stop working properly after a certain number of years, is part of the reason such problems occur.

Many tech companies, such as Apple, do not promise users a smooth experience for customers after they have owned a device for several years.

“Some companies have been proactive about educating customers about this problem, and some companies got lazy and didn’t do their homework and expect customers to figure it out on their own if issues start occurring on older devices,” said Leonard Grove, CEO of SSL.com, a well-known private commercial provider of digital certificates.

Although there is a significant risk of millions of devices not working on Thursday, some internet security experts say it could affect every device in a different fashion.

“We just don’t know what exactly will happen, it could be like Y2K in 2000 with a big warning and nothing happens, or you could see a lot of people rushing to fix their devices or getting new ones,” Grove added.