Issued 8/16/18

Open Sesame Bug Allows Anyone to Hack Windows 10 Using Just Their Voice

A vulnerability called Open Sesame allows hackers to execute arbitrary code on a Windows 10 computer using just their voice. The bug exists in digital assistant Cortana, and a team of researchers revealed at the Black Hat conference in Las Vegas that anyone could get rights to access sensitive files, connect to malicious websites, download and run infected files, and even gain elevated privileges on a locked computer. It's all possible due to the fact that the UI on Windows 10 now allows apps to run in the background, and while the computer is locked for mouse and keyboard use, Cortana can still perform a series of tasks. Security researchers Amichai Shulman, Tal Be'ery of Kzen Networks, and Ron Marcovich and Yuval Ron of the Israel Institute of Technology discovered the flaw and reported it to Microsoft back in April, according to a report from ThreatPost. "An Elevation of Privilege vulnerability exists when Cortana retrieves data from user input services without consideration for status. An attacker who successfully exploited the vulnerability could execute commands with elevated permissions. To exploit the vulnerability, an attacker would require physical/console access and the system would need to have Cortana assistance enabled," Microsoft explains. The flaw exists in Windows 10 Fall Creators Update (version 1709) and April 2018 Update (version 1803) and newer and installing the most recent update keeps systems protected.