# Cortana vulnerability has been patched

14 June 2018, by Nancy Owano

Microsoft has a security update regarding Cortana and it's worth a look.

CVE-2018-8140 is all about "Cortana Elevation of Privilege Vulnerability."

The vulnerability is "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."

For the exploit to succeed, though, the attacker would need physical/console access—and the system would need to have Cortana assistance enabled.

So what's the update about? The vulnerability is addressed "by ensuring Cortana considers status when retrieves information from input services."

This story starts with June's "Patch Tuesday" (June 12) and when it arrived one could swear the music carried muffled alarm bells.

Patches in this cycle fixed a code execution vulnerability using the default settings for Windows 10 and the Cortana voice assistant. In techie lingo, we are looking at an issue of discovering a "Cortana lock screen bypass bug in Windows 10."

McAfee engineer and security architect Cedric Cochin and Steve Povolny, who heads advanced threat research there, wrote about Windows 10's Cortana issue. They walked readers through what happened.

"Personal digital assistants such as Siri, Alexa, Google Assistant, and Cortana have become commodities in many technologically inclined houses," they wrote, and they reported to Microsoft several issues about Cortana. Reports said they disclosed details of the issue to Microsoft in April.

The Cochin and Povolny team noted that "A team of several independent researchers also discovered and disclosed this vulnerability around the time of our submission. Additional credit for this discovery goes to: Ron Marcovich, Yuval Ron, Amichai Shulman and Tal Be'ery."

While the two provided an interesting detailed account of what was identified as vulnerable points, Darren Allan in *TechRadar* provided a succinct take-home of what was the big deal: "you could trigger the voice assistant from the lock screen (assuming Cortana is enabled in this respect, on default settings), and bring up a contextual Windows 10 menu simply by typing while Cortana is listening to a query."

Yes, Microsoft has patched the issues.

"In Windows 10, on the most recent build at the time of submission, we observed that the default settings enable 'Hey Cortana' from the lock screen, allowing anyone to interact with the voice-based assistant. "

The two said this led to vulnerabilities that allowed arbitrary code execution. They said typing while Cortana starts to listen to a query on a locked device will bring up a Windows contextual menu.

(Cue in pained smile.)

"We now have a contextual menu, displayed on a locked Windows 10 device," they said. "What could go wrong?"

*Windows Central* said, if executed correctly by the hacker, "hackers could use Cortana from the lock screen to run PowerShell scripts or load malicious software from a USB stick." Dan Thorp-Lancaster said, "Researchers were also able to use the exploit to perform a password reset and gain full access to the machine."

They could hover over any relevant match. If the match is driven by filename matching, then you would be presented with the full path of the file. "If the match is driven by the file content matching, then you may be presented with the content of the file itself."

The McAfee pair proceeded in further detail about their examination of Cortana, and in closing they made the particularly important point. "The attack surface created by vocal commands and personal digital assistants requires much more investigation; we are just scratching the surface of the amount of research that should be conducted in this critical area."

**More information:**
securingtomorrow.mcafee.com/mc … rtana-cve-2018-8140/


APA citation: Cortana vulnerability has been patched (2018, June 14) retrieved 22 September 2021 from https://techxplore.com/news/2018-06-cortana-vulnerability-patched.html