

RAVENii News

Not Your Typical Patch Tuesday

On Tuesday, April 14, 2020 Microsoft fixed 113 security vulnerabilities in its various Windows operating systems and related software. Three are actively being exploited. Two others have been detailed to the public prior to the release. Nineteen were assigned Microsoft's most-dire "critical" rating.

You can read the article from Krebs on Security here:

<https://krebsonsecurity.com/2020/04/microsoft-patch-tuesday-april-2020-edition/>

The moral of the story is to make sure you are up to date on your patches and make sure your patching process includes backing up critical files before attempting these patches.

If you are a member of RAVENii's Security Patch Program, your patches have been deployed per your requirements. Michael Yelland, RAVENii CSO says, "We are aware of the vulnerabilities. If RAVENii does your patching, we want you to know that we are applying patches as defined in our agreement with you."

It also comes highly recommended per the top 20 CSC controls to continuously scan your network for vulnerabilities and missing patches. It is a checks and balances for your patching program.

"Due to the coronavirus, our business landscapes had to change whether we were prepared for it or not. This leaves us more exposed as the workforce shifts from the office to the home," says Yelland. "It is extremely important to be diligent with keeping your systems up-to-date with security patches now more than ever."

If you need help putting a plan together or refining the process you have in place, we are here to assist. Don't hesitate to reach out. Together we conquer.

Stay Safe and Be Well!