Patch Tuesday, the second Tuesday of every month, marks the day that Microsoft releases a cluster of security patches for its operating systems and other software. IT managers often brace for Patch Tuesday with a mixture of fear and suspense. Here’s why:

The Cost of Poor Patching
In the last year, 70 global enterprise organizations lost...

- $400 million from 2,122 data breaches
- 700 of their records were compromised in 79,790 security incidents

More than 70% of attacks exploited known vulnerabilities with available patches.

Zero-Day Forever

July 14, 2020: Microsoft will discontinue patch releases for Windows 7.

Other Problems with Patches

Exploit Wednesday
Day after Patch Tuesday. While IT tests patches before deploying them, hackers swoop in with new zero-day exploits.

Patches? What Patches?
Hackers can now reverse-engineer patches to create new exploits in a matter of days, if not hours.

30 Days of Night
If an attack is mounted soon after Patch Tuesday, hackers could have an entire month to exploit the vulnerability if Microsoft doesn’t release an emergency patch.

Other Problems with Patches

Legacy Apps
Businesses stuck with older versions of Java, Reader, and Flash are vulnerable to attacks via web browsing or phishing emails.

BRICK HOUSE
A few recent patch releases have caused problems on the day they are installed—at minimum requiring an uninstall and additional maintenance. Some are so problematic, they totally brick the computer.

Learn more about how to protect vulnerable software at malwarebytes.org/business.