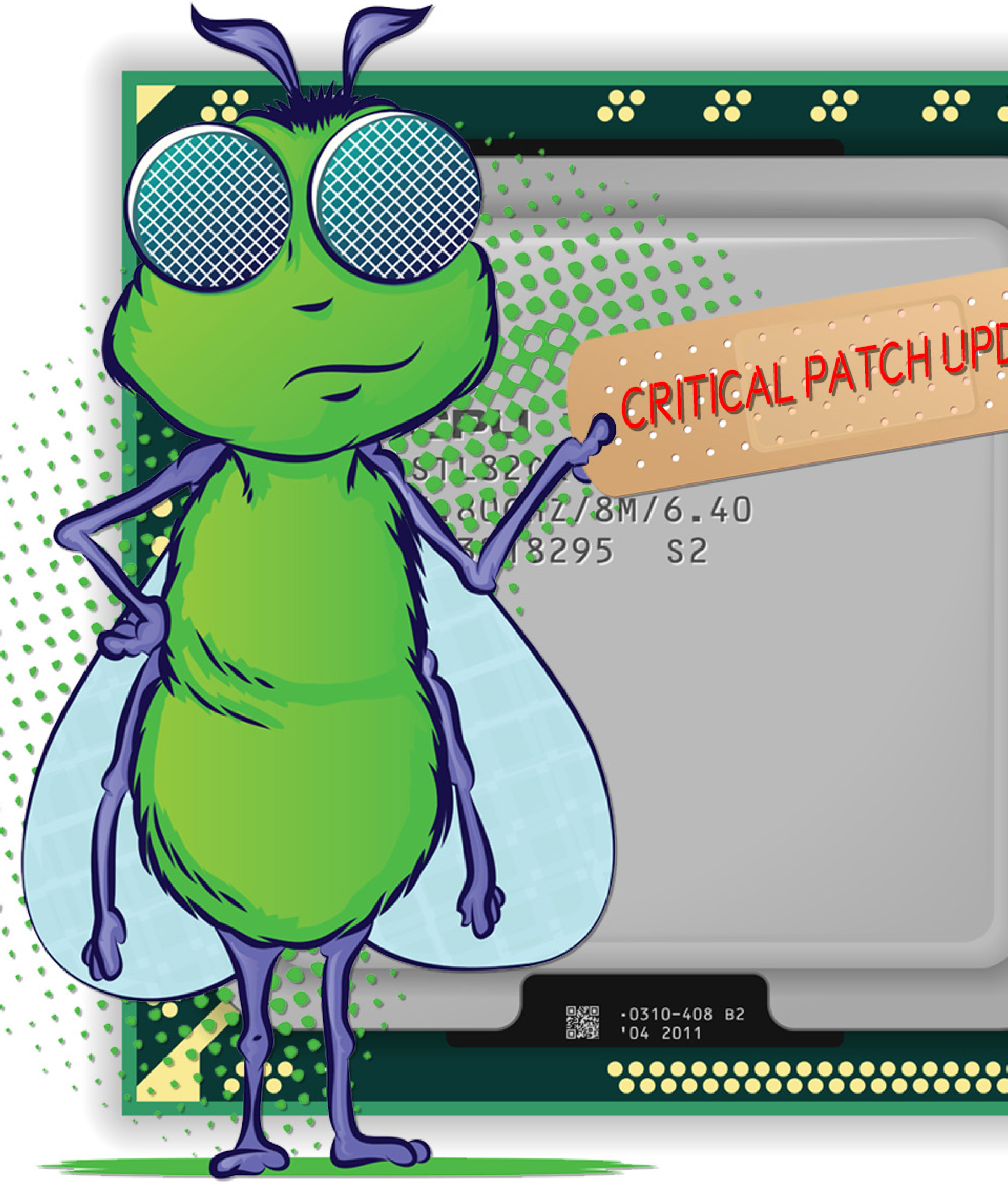
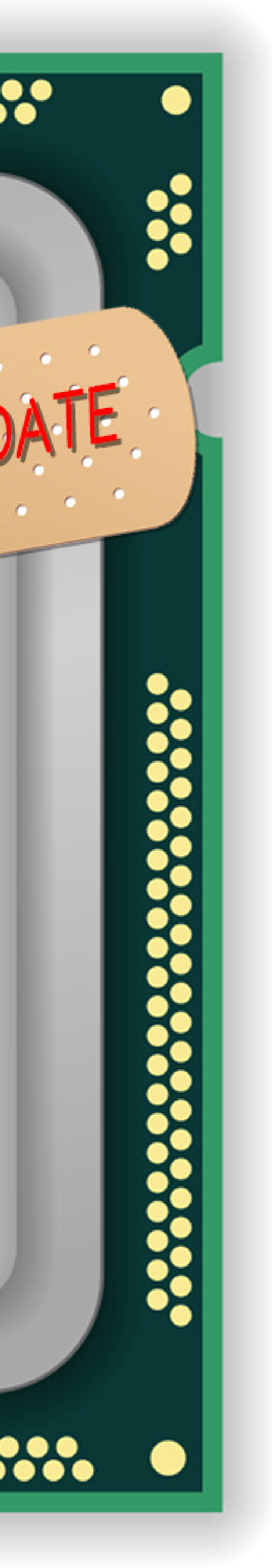

CRITICAL PATCH UPD
CPU
STL820
800GHZ/8M/6.40
8295 S2
-0310-408 B2
'04 2011



BREAKING NEWS: BIGGEST, BADDEST CPU BUGS EVER!

By Paul O'Neal, President, International Networking, Inc.

Recently, there has been disturbing news regarding CPU (Central Processing Unit) bugs that attack most all computing devices (such as PC's, Laptops, Tablets, SmartPhones, SmartWatches, etc.) that run 3rd party apps. The manufactures most mentioned include Intel, AMD and ARM. These computing devices have proven to be extremely vulnerable to attacks referred to as ***Spectre*** and ***Meltdown***. These are two separate vulnerabilities allow different, but potentially harmful methods of attack that strategically target the CPU.

Intel is expected to have a fix, by January 14, 2018, for 90% of their processors made in the last five years with more updates to follow later this month. You can find more information about the Intel fix here. Since the beginning of the year there has been an overwhelming amount of news and updates regarding these attacks through mainstream channels. Laura Hautala, with CNET wrote an outstanding article which confirms as of January 8, 2018, Apple has released their patches, Apple iOS 11.2.2 and macOS 10.12.2. If your device is compatible with either of these versions you shouldn't hesitate to update your device(s) immediately.

Microsoft released an update for Windows 10 on January 3, 2018 and is expected to release their patches for Windows 7 and 8 on January 9th, 2018. A very important side note, Microsoft updates will not get applied unless the registry is updated by your AV software. For more on Microsoft updates follow this link.

The newer/newest Google phone has already been patched and newer/newest Android phones are expected to be patched soon. It should be noted; older versions of Android Tablets and phones may never be updated.

We now know this CPU vulnerability has actually been around since 1995 and consumers are just now hearing about it.

As you would direct your patients during the treatment of their care, it is important to follow the development of these CPU bugs as they have been labeled as "not easy to fix." The post CPU "update" symptoms can include: broken updates, performance decline, as well as, other operating issues, which is why it is recommended (and to stress for high-priority security reasons), you apply all applicable patches at your earliest convenience while continuing to monitor your systems performance and watch for more updates to be released.

Lastly, this article only begins to scratch the surface of an extremely volatile computer bug. Staying informed and further research as to how these bugs can affect you and your practice is highly recommended. Also, take the time to read Laura Hautala's article. She addresses vulnerabilities, fixes, questions and best protection methods—basically everything you need to know about these vicious bugs. §

Taken from Google's Whitepaper

This is Meltdown:
First, an attacker makes the CPU execute a transient instruction sequence which uses an inaccessible secret value stored somewhere in physical memory. The transient instruction sequence acts as the transmitter of a covert channel, ultimately leaking the secret value to the attacker."

And here's Spectre:
Spectre attacks induce a victim to speculatively perform operations that would not occur during correct program execution and which leak the victim's confidential information via a side channel to the adversary.