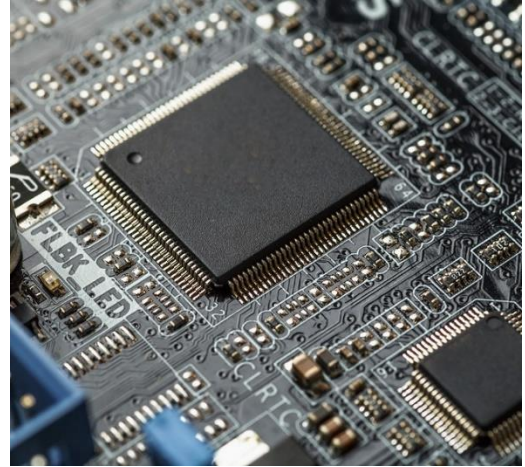# eMazzanti Technologies Offers Updates to Patch Meltdown and Spectre Security Flaws

NYC area IT security consultant helps customers protect their computer and device processors from attacks exploiting the Meltdown and Spectre vulnerabilities

Hoboken, New Jersey -- (Cision) January 9, 2018 — eMazzanti Technologies, a NYC area IT security consultant and MSP, issued emails over the weekend warning customers about the recently publicized Meltdown and Spectre security flaws that affect countless personal, business, cloud and mobile computer processors worldwide.

In the urgent communication, the company explains the nature of the Meltdown and Spectre vulnerabilities and countermeasures that software giants Microsoft and Apple are undertaking to prevent exploitation of the flaws. eMazzanti then offers to help customers "patch, backup, and install the latest software" to keep their environments up and running.

The email notice also provides a link to a Meltdown and Spectre technical analysis of what these two vulnerabilities could mean to a customer's infrastructure.

"eMazzanti Technologies has been working tirelessly with our partners and hardware vendors to ensure that our client base has taken the appropriate steps to protect their data.," stated Almi Dumi, Chief Information Security Officer, eMazzanti Technologies. "We urge customers with any questions or concerns to contact us by calling our service desk at (201) 360-4400 or submit a support request by email."

Meltdown and Spectre Warning

Here is the text of the email warning:

"Chances are you own a smartphone or computer that contains a chip that hackers could potentially exploit to get access to sensitive information.

That's because billions of devices are affected by two major security flaws revealed by cyber-security researchers on Thursday. The flaws, dubbed Meltdown and Spectre, affect processing chips made by Intel, AMD and ARM Holdings. That means if you use a desktop, laptop, smartphone or cloud service from Apple, Google, Amazon, or Microsoft you might be vulnerable!

It is important to note that the exploitation of either one of the vulnerabilities is virtually untraceable and almost impossible to detect. The attacks leverage technologies developed to improve performance

on processors affecting millions using personal and cloud computing as well as mobile devices such as smartphones.

As a countermeasure to Spectre and Meltdown software companies such as Microsoft and Apple have rolled out patches to protect against side-channel attacks and prevent kernel space and physical memory mapping available in user space.

We can help you: patch, backup, and install the latest software to keep your environment up and running. Don't wait for it to happen to you, contact us at help@emazzanti.net or call us 24/7 at 866-360-4400."

Staying Vigilant

Keeping up with threats to sensitive data requires that individuals and organizations stay vigilant. Accordingly, anyone charged with data security who is unsure about what to do may call the IT security professionals at eMazzanti Technologies

Related resource information:

Stick with Security: Secure remote access to your network

Tips to Improve Your Cybersecurity in 2018

About eMazzanti Technologies

eMazzanti's team of trained, certified IT experts rapidly deliver retail and payment technology, digital marketing services, cloud and mobile solutions, multi-site implementations, 24×7 outsourced network management, remote monitoring and support to increase productivity, data security and revenue growth for clients ranging from law firms to high-end global retailers.

eMazzanti has made the Inc. 5000 list eight years running, is a 2015, 2013 and 2012 Microsoft Partner of the Year, 2016 NJ Business of the Year, 5X WatchGuard Partner of the Year and one of the TOP 200 U.S. Microsoft Partners! Contact: 1-866-362-9926, info@emazzanti.net or http://www.emazzanti.net Twitter: @emazzanti Facebook: Facebook.com/emazzantitechnologies.