February 2018

TechTidbit.com

brought to you by Tech Experts

Meltdown and Spectre: Protect Yourself With Updates

Jason Cooley is Support Services Manager at Tech Experts.

As I am writing this, it has been about a month since news broke of Meltdown and Spectre, two separate vulnerabilities affecting nearly every smartphone and PC in use today. It affects all modern processors – which encompasses a whole lot of users.

Meltdown and Spectre are different fundamentally, but they use a similar vulnerability to do different things. So what are the differences?

Meltdown breaks the isolation between user applications and the operating system.

This allows a program to access the memory and, therefore, the processes and data of the software, even when it is not authorized to do so.

Meltdown specifically affects Intel x86 microprocessors and some ARM-based microprocessors. Many different systems are affected, including iOs, Linux, macOS, and Windows, as well as a wide range of cloud services and servers across the world.

Spectre, however, breaks the isolation between different applications. It allows an attacker to trick programs into leaking their secrets and data. It can easily jump to other programs after it has made its way in.

While Spectre is harder to exploit than Meltdown, it is also harder to defend against.

Spectre can affect any microprocessor that runs branch prediction, which is the processor trying to predict what you will do next and begin running background processes to allow for faster performance.

It has been confirmed to affect both Intel and AMD. AMD, whose processors are immune to Meltdown, have already been experiencing many issues due to security patching.

Now you know what they are, but what can you do to stay safe?

Keep your device up to date. Right now, it is as simple as that. Processors won't be replaced for a more secure model, but updates can shield users from the exploits.

Microsoft has rolled out updates to battle the vulnerabilities for both Intel and AMD processors. Apple has pushed iOS updates. Browsers are being updated, and so is software.

While we have updates to close up the holes, initial reports coming in state the patch has a negative impact on system and processor performance.

Microsoft put a patch out to fix the vulnerability for AMD processors and essentially broke most systems running Windows with an AMD. They had to remove the patch from their updates.

Companies are scrambling to get fixes in place, ones that will affect us as little as possible.

While it is unfortunate that system performance may suffer due to the patching, it is better than the alternative of leaving yourself unprotected and vulnerable to hackers.

Experts estimate it won't be long before hackers have processes in place to take advantage of these vulnerabilities, so everyone is working to have a fix in place before that happens.

While we may suffer performance-wise for the time being, tech giants like Microsoft and Intel will continue looking for better solutions.

Putting a fix in place that slows down performance does not mean a future patch will address that. It's just the price of being safe and one we will all have to pay.

Experts estimate it won't be long before hackers have processes in place to take advantage of these vulnerabilities, so everyone is working to have a fix in place before that happens.

Windows Updates: Allow Them, Don't Block Them

"There are always going to be people doing nefarious things when it comes to computers and the Internet, but the engineers behind your operating system and your antivirus company will always be on top of a fix for the vulnerability as soon as it is discovered."

Ron Cochran is Help Desk Supervisor at Tech Experts.

One of the first things you should do when purchasing a new computer (or rehabilitating an older computer) is to make sure the operating system is up-to-date with the latest security patches. In some cases, people disable the automatic updates and this can cause a whole host of issues.

Microsoft regularly puts out security patches, as well as other patches for their software. These patches are applied through the automatic update process. When that process is disabled, this means your computer hasn't received the latest updates from Microsoft. Because your updates are halted, the system vulnerabilities that Microsoft engineers have found have not been repaired on your system.

You may remember the WannaCry Ransomware attack or, by now, heard of the most recent news of the Intel CPU flaw with Meltdown and Spectre. These two vulnerabilities, if exploited, can wreak havoc on an affected computer. An affected system could suffer circuit issues, data corruption, system instability, and even data theft.

There are always going to be people doing nefarious things when it comes to computers and the Internet, but the engineers behind your operating system and your antivirus company will always be on top of a fix for the vulnerability as soon as it is discovered.

Did you know that Microsoft releases most Windows Update patches on "Patch Tuesday" – the second Tuesday of each month? This keeps automatic system reboots to a minimum and also assists managed service providers like Tech Experts in ensuring that all of their clients' servers and workstations have the latest software and security patches installed.

At home, you can set your Windows Updates to the "Automatic" option. That way, your system will automatically check for Windows Updates every 24 hours or so if the computer is connected to the Internet.

If you're thinking to yourself, "I just use my home computer for browsing DIY pages, listening to music, and sending emails. Why would anyone want to get into my computer?," reconsider how much personal information is actually stored.

It may seem as though your computer wouldn't hold much useful information, but a hacker only needs a few passwords, an email address, phone number, and address to potentially gain access to cell phone accounts, shopping site accounts, tax information, and even banking and credit card accounts.

Even if the hacker isn't looking for personal information like that listed above, they could still use your computer to send spam emails to other computers all over the world, slowing down your computer and Internet and causing a whole slew of issues for other computer owners.

Keeping your operating system up-to-date with the latest updates and security patches, keeping your anti-malware and anti-virus software updated and running on a regular basis, and adding robust security settings to your router and firewall will help keep all of these vulnerabilities behind closed doors. At least, until the software engineers can create and deploy the patches and updates to block access to them.

What's The Difference Between Internet, Intranet, & Extranet?

The terms intranet, Internet, and extranet are often used interchangeably; however, there are some important differences between them. To better understand these differences, it is useful to look at the prefixes.

The prefix intra means within, inter means between, and extra means beyond. So how does this translate to online-based networks?

Basically, the Internet is an open entity that anyone in the world can access. It is open to everyone who has a working computer or device and appropriate Internet access. An intranet is a private network that is typically limited to authorized users.

For example, most major organizations operate some form of intranet that only employees of the business can access and use. Intranets are usually employed to support a corporate culture and objectives and provide a platform on which employees can share information, communicate, collaborate, and network. They are generally faster than the Internet because the information is stored on local network servers as opposed to being accessed from data centers throughout the world.

An extranet combines some elements of both the Internet and intranet. It is open to people both within and outside an organization; however, only people who have prearranged authorization can access it. An extranet is a restricted network that some, but not all, members of the public can access. A company may develop an extranet to create a mechanism by which it can connect with suppliers, customers, and other external agencies without making the content visible to the general public.

How To Protect Your Computers From Electrical Anomalies

Chris Myers is a field service technician at Tech Experts.

Many people will recognize these as risks of a power outage that can damage computers, but did you know that there are actually many different types of power anomalies? If the power dips for even a quarter of a second (250 milliseconds), your computer will use up its reserves of power and abruptly shut down after only 17 milliseconds.

Types of electrical anomalies

Sags, also known as brownouts and undervoltage, are temporary decreases of voltage levels. This is a very common problem, making up a majority of the power disruptions your computer will encounter. When a sag happens, computers may not get enough voltage to power all of its components. This can cause unseen data corruption, power loss to fans, and a freezing keyboard or mouse.

Electric companies purposefully induce sags in order to deal with periods of high power demands, such as high usage of air conditioners on a hot day.

Blackouts are when all power is lost. They are typically caused by power grid equipment failure, lightning, ice, car accidents, and natural disasters. When a blackout occurs, all data in your RAM and hard drive caches is lost. If critical system files like the File Allocation Table are damaged, it may render your hard drive inoperable.

A spike, also called an impulse, is a sudden and dramatic increase in voltage usually lasting less than one millisecond. It can be caused by a lightning strike or a large section of network equipment coming online. Spikes can cause catastrophic damage to computers, often overloading power supplies and burning circuit boards.

A surge, also referred to as a transient, is a short period of increased voltage typically lasting between 8 milliseconds and 2.5 seconds.

Depending on the voltage, surges can cause damage similar to that of spikes.

Noise refers to both Electro-Magnetic Interference (EMI) and Radio Frequency Interference (RFI). Electrical power is transmitted with sine waves, usually as an alternating current (AC). The usage of many electronic devices in close proximity to each other can alter the pattern of these waves. When this occurs, it can result in overheating, data loss, and distorted audio or video.

Frequency shifts, also known as harmonic distortion, usually happen when lighting equipment shifts the sine wave frequency to something other than the standard 60 Hertz. This can result in the overheating of electrical wiring and power supply errors leading to unscheduled shut downs.

Preventing damage

Surge protectors are the easiest and most affordable way to provide your equipment with an immediate layer of protection. When buying a surge protector, you want a high amount of joules and low let-through voltage.

Joules are basically how much energy the device can absorb over its lifetime. Let-through voltage is how much voltage is passed on to connected devices when the surge protector is hit with a 6,000-volt surge.

The best surge protectors will even have outlets for phone, TV, and USB cables. All of those cable types can be damaged from power surges. Just make sure you aren't getting a power strip string only, which is simply an extension of a wall outlet and offers no protection.

For the best protection you will need an uninterruptible power supply (UPS).

These power supplies will provide power to your equipment whenever it sags or stops completely. Most small power supplies will keep your computer running for about 10 minutes or just network equipment for about an hour. Having enough time to properly shut down your equipment can mean all the difference when it comes to saving your data and hardware.

"The best surge protectors will even have outlets for phone, TV, and USB cables. All of those cable types can be damaged from power surges. Just make sure you aren't getting a power strip string only, which is simply an extension of a wall outlet and offers no protection."

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Important Aspects Of Cybersecurity

Evan Schendel is a help desk specialist at Tech Experts.

In this age where dangers lie around every digital corner on your computer, what could possibly keep everyone safe and secure?

Cybersecurity experts are the first line of defense and are quite good at holding that line. These experts protect many fields ranging from hardware and software to sensitive data and financial information, even users themselves.

Hardware and software

The maliciousness of viruses can cripple whole systems and a countless number of links or applications can deliver dangerous viruses or malware. These viruses and dangers evolve every day.

Hardware can be manipulated by vulnerabilities and exploitations as well. Without intention of frightening you, each part of your computer could be of interest to the right person, as the recent Meltdown and Spectre issues have shown. It isn't simply your operating system or data that can be affected.

This constant cycle of attacker-and-defender leaves thousands of unfilled jobs for cybersecurity and the protection of devices. If these jobs were not filled or properly trained, computer systems across the world would fall prey to hackers. However, your device itself is not the only thing that can be harmed.

Sensitive data and users

When unauthorized hands gain access to personal information, it can lead to disaster. A person's financial and personal data is important and the people who protect that data are far fewer than those seeking it out.

Anti-virus programs are made by people who know viruses well, often those who had created viruses or malware prior to their more noble ventures.

These should always stay updated and definitions for these pieces of software tend to be updated with frightening frequency. Staying up-to-date on malicious software and code is the only real method of stopping it, after all.

Systems administrators also have the need for people who can spot discrepancies or potentially malicious actions in their networks and keep standards up to snuff. Passwords and safety precautions must be set to a standard that is important to follow and uphold.

Information over the phone can also be an issue, as many users have trouble distinguishing a scammer from a legitimate caller. This is where education and prevention come in.

Educating people about how potential scammers may work is one of the most important aspects in preventing unsuspecting folks from giving their credit card information away, or worse.

Preventing these scammers from calling thousands of people a day is also of utmost importance, but requires experts and trained technicians (even the government, in some cases) to crack down on these cyber criminals.

Lastly, the most vulnerable aspect of a computer's security is, unfortunately, the user. Tricky emails and legitimate-looking sites can be incredibly tough to distinguish from the original product. Most wouldn't even suspect such an uncanny replication.

This is where user error molds with a criminal's savvy nature. If this sounds unrealistic to fall for, then it's even better, but more times than not, someone will fall for it – even the experts can be fooled by sophisticated trickery or maybe a simple lack of awareness.

Luckily, if this is the first issue, the other sections can come into play and protect your systems and yourself from being subject to data loss or cyber-thievery.