Monthly Cybersecurity Newsletter

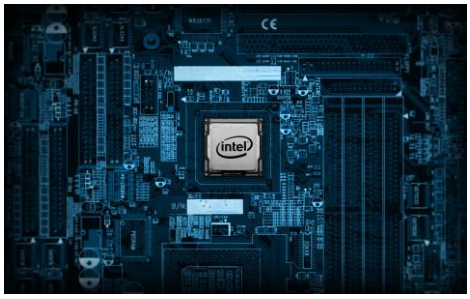
January 2018
Issue

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

---

Happy New Year…Your Computer is Vulnerable!



Most people have probably heard about the new vulnerabities affecting almost every modern computing processor. A security research team from Google Project Zero reported on January 2, 2018 two vulnerabilities that potentially impact all major central processing units (CPUs). These "new" vulnerabilities were known inside the chip and software industry since the middle of 2017, and are deeply embedded in the fundamental design of processors. The vulnerabilities are called Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5753 and CVE-2017-5715). Both vulnerabilities leverage a feature found in most modern CPUs called "speculative execution" that is used to optimize performance.

While computer programs are typically not permitted to read data from other programs, malicious programs can exploit Meltdown and Spectre to steal data stored in the memory of other running programs. This could include passwords, personal photos, emails, instant messages and documents. Meltdown breaks a fundamental isolation between *user applications and the operating system (OS)*, allowing an application to access all system memory, and thus the secrets of other programs and the OS. Almost any computer is vulnerable to a Meltdown attack. Spectre breaks the *isolation between different applications* and allows an attacker to trick programs into leaking data. Any safety checks a program may have actually increases the potential for attack and may make the program more susceptible to Spectre. A Spectre attack works on almost every system, including desktops, laptops, smartphones, and servers in the cloud. It is also hard to mitigate because it requires changes to processor architecture to fix it.

The main OS vendors have rushed to provide security patches to protect their systems from these attacks. Software patches at the OS level have largely mitigated the Meltdown flaw, but both Microsoft and the Linux community said a firmware fix would be necessary to fully address the Spectre vulnerability. Processor manufacturers have started releasing firmware updates for processor models affected by Meltdown and Spectre. Fixes are being integrated into BIOS/UEFI updates for affected PCs. While not all vendors currently have patches available for vulnerable products, most have promised updates in the near future. The good news for now is there are currently no reports of these vulnerabilities being exploited remotely. According to one anti-virus vendor, however, cyber-criminals are capitalizing on Meltdown and Spectre in order to trick users into downloading malware disguised as security patches. Therefore, individuals need to remain vigilant and install updates only through normal vendor channels.

January 28th, 2018 will be ***Data Privacy Day***. It is an event that began in the United States and Canada in January 2008 as an extension of the European Data Protection Day. Data Privacy Day is designed to promote greater awareness about the importance of privacy and protecting personal and sensitive information. It is observed annually on January 28.

The National Cyber Security Alliance (NCSA) officially leads the Data Privacy Day campaign and tries to align the campaign with the most current privacy issues in a thoughtful and meaningful way. NCSA's privacy awareness campaign is an integral component of STOP. THINK. CONNECT. ™ – the global online safety, security and privacy campaign. For more information about Data Privacy Day, including a list of events and resources related to it, please visit the following site: https://staysafeonline.org/data-privacy-day/about/.

Attached to this newsletter is an infographic the ESRMO encourages you to share among your staff and colleagues in order to promote Data Privacy Day. One way to help protect private information is to properly dispose of documents and other items when sending government/ business property to surplus. Some of the most common areas where confidential material is found are in desks and filing cabinets that were not properly searched. It is important that all surplus items are thoroughly inspected to ensure that they contain no confidential information before they are ever removed from the facility. Together we can raise awareness to the importance of protecting sensitive information, at home, at work, and in our communities.

Keep Us All Safer by Securing Your IoTs!

Many people have now heard about the "Internet of Things" (IoTs), which are really any electronic device that connects to the Internet. IoT devices can be anything from security cameras, routers, and refrigerators to printers, wearable devices, "smart" plugs and "smart" lightbulbs. IoTs add convenience to our lives, but they can also make us more vulnerable to attack. Throughout 2016 and 2017, attacks from massive botnets (networks of devices that are infected with malicious software and controlled as a group without the owners' knowledge) were comprised of hacked IoT devices. A botnet called Mirai disrupted the Internet in 2016 by compromising poorly secured IoT devices and using them for large cyberattacks on other networks. Because of IoT-based attacks, experts warn of a dire outlook for Internet security; however, the future does not have to be so bleak. IoT attacks should remind us how important it is to secure these convenient devices. The following advice may reduce your chances that IoTs become a liability for you and for others:

- Do your research! Ensure that the IoT manufacturer takes cybersecurity seriously.
- Disable Internet access for devices that do not need Internet access.
- Place your devices behind a firewall on your network.
- Change default account names and passwords on all network devices.
- Download and install the latest firmware updates, *and* keep your devices updated.
- Avoid devices that advertise Peer-to-Peer (P2P) capabilities built-in.
- Turn off IoT devices when they are not in use or not needed for a period of time.

For more information on how to secure IoTs, take a look at the advice published by the Department of Justice (DOJ) titled "Securing Your Internet of Things Devices":

https://www.justice.gov/criminal-ccips/page/file/984001/download

---

Don't forget the other **monthly newsletters** available to you! The following are the various cybersecurity newsletters the ESRMO distributes each month. We hope you find them beneficial.

- **SECURITYsense Newsletter:** A licensed newsletter for State employees that contains several articles involving current cybersecurity issues. **Note:** *You must have a Microsoft O365 account with access to the ESRMO external SharePoint site to access this resource*.

https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/SECURITYsense

- **Security Tips Newsletter:** A free monthly cybersecurity newsletter from the Center for Internet Security (CIS). This month's edition is on ***National Data Privacy Day, January 28th***.

https://www.cisecurity.org/resources/newsletter

- **SANS OUCH! Newsletter:** A free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Creating a Cybersecure Home.***

http://securingthehuman.sans.org/resources/newsletters/ouch/2017

FEMA Emergency Management Institute - Weekly EMI e-Forums - Wednesdays 3:00 – 4:00 p.m. EDT

You are invited to join the FEMA EMI e-Forums, which are 1-hour, moderated, webinar discussion forums that provide an opportunity for EMI and the emergency management community to discuss matters of interest on national preparedness training and exercise. EMI e-Forums facilitate a discussion of whole community-presented best practices. The panel members are whole community, with topics relevant to whole community. These exchanges of ideas are free of charge and available to anyone who wishes to participate. Upcoming topics are below:

2/7.....An Emergency Management Reference Guide for Elected Officials

2/14....Training and Exercise Planning Workshop: Best Practices for Preparation

2/21....Healthcare Facility Emergency Management. Best Practices in Healthcare Community

2/28....X, Y, Z Learning: Bridging the Gap in Multigenerational Classrooms

Login link: https://fema.connectsolutions.com/emieforums

Conference call-in: 800-320-4330, PIN 107622

Have you considered **FedVTE**? The Department of Homeland Security (DHS) provides the FedVTE program, a free, on-demand, online cybersecurity training program with 24/7 accessibility. DHS offers FedVTE courses at no cost to government staff, including contractors. With 60+ courses at varying levels of proficiency – from beginners to advanced – all cybersecurity professionals, aspiring and current, can build skills specific to their interests, work roles, and professional goals. Courses are added or updated on a rolling basis.

KEY FEATURES:

- ✓ Access **24/7**
- ✓ Over **60+** available courses of varying proficiency – beginner to advanced
- ✓ Self-paced
- ✓ Many popular certification courses including:
  - Network +
  - Security +
  - Certified Information Systems Professional (CISSP)
  - Windows Operating System Security
  - Certified Ethical Hacker (CEH)
- ✓ All courses are aligned to the NICE Cybersecurity Workforce Framework
- ✓ Individuals can take courses to build the required knowledge, skills, and abilities in the cybersecurity field
- ✓ Taught by experienced cybersecurity subject matter experts

For more information and to visit FedVTE, please go to https://fedvte.usalearning.gov.

Upcoming Events…

- ➢ **January 28, 2018** – National Data Privacy Day
- ➢ **January 30-31, 2018** – *NIST Risk Management Framework* training @ 3900 Wake Forest Rd., Raleigh NC.
- ➢ **February 20, 2018** – Quarterly Security Liaison Meeting

---

Do you have something to share? Is there a topic you would like to see in a future newsletter? The ESRMO encourages staff to share topics that will be of value to all agencies in order to foster better information sharing and awareness. If you have a suggestion for a topic that you would like for us to consider for a future newsletter, please send it to security@its.nc.gov.

DATA PRIVACY DAY **JANUARY 28, 2018** #PrivacyAware

DATA PRIVACY DAY

is an internationally recognized day dedicated to creating awareness about the importance of privacy and protecting personal information.

CREATING A GLOBAL COMMUNITY THAT RESPECTS PRIVACY, SAFEGUARDS DATA AND ENABLES TRUST BEGINS WITH YOU!

STOP. THINK. CONNECT.™ is simple, actionable advice you can use to educate people about privacy at home, at work and in your community.

AT HOME

TALK WITH YOUR FAMILY AND FRIENDS ABOUT WAYS TO STAY SAFER ONLINE.

PERSONAL INFORMATION IS LIKE MONEY. VALUE IT. PROTECT IT.

Be thoughtful about how your personal information is collected through apps and websites.

OWN YOUR ONLINE PRESENCE

Learn about and use privacy and security settings on your favorite online games, apps and platforms.

AT WORK

HELP ALL EMPLOYEES UNDERSTAND THE ROLE THEY PLAY IN MAKING SURE PRIVACY IS ACHIEVED AND MAINTAINED.

WHEN IN DOUBT, THROW IT OUT

Links in emails, social media posts and online advertising are often how cybercriminals steal personal information. Even if you know the source, if something looks suspicious, report it or delete it.

PRIVACY IS GOOD FOR BUSINESS

Engage employees with initiatives such as lunch and learns, funny videos and competitions.

IN YOUR COMMUNITY

SHARE YOUR PRIVACY KNOWLEDGE BY VOLUNTEERING IN A LOCAL SCHOOL, SENIOR CARE FACILITY OR FAITH-BASED ORGANIZATION. USE FREE RESOURCES FROM STAYSAFEONLINE.ORG TO SPREAD THE WORD.

SHARE WITH CARE

Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it could be perceived now and in the future.

BE PART OF SOMETHING BIG!

#ChatSTC

Join us on Wednesdays in January (Jan. 10, 17 and 24) at 3 p.m. EDT/ noon PDT using the hashtag #ChatSTC.

DATA PRIVACY DAY CHAMPION

Register yourself and/or your company as a Data Privacy Day Champion.

#PrivacyAware

Use #PrivacyAware on social media and follow us on Facebook (/StaySafeOnline), Twitter (@StaySafeOnline) and Instagram (@PrivacyAware).

FOR FREE RESOURCES AND TO LEARN MORE, VISIT STAYSAFEONLINE.ORG/DATA-PRIVACY-DAY/

NATIONAL CYBERSECURITY ALLIANCE

@STAYSAFEONLINE
/STAYSAFEONLINE

STOP | THINK | CONNECT™

The National Cyber Security Alliance officially leads Data Privacy Day in North America. STOP. THINK. CONNECT.™ is the global online safety campaign to help everyone stay safer and more secure online.