NEWS BRIEF

Critical Cyber Exploits Affect Nearly All Computers

Cyber security researchers recently announced the discovery of two major security flaws that could allow hackers to bypass regular security measures and obtain normally inaccessible data. The flaws, referred to as **Meltdown** and **Spectre**, are both caused by design flaws found in nearly all modern processors. These vulnerabilities can be exploited to access all of the data found in personal computers, servers, cloud computing services and mobile devices.

Because Meltdown and Spectre are both caused by design flaws, experts believe that they will be harder to fix than traditional security exploits. Additionally, software patches that have already been released to help address the vulnerabilities can cause computer systems to slow down significantly, which may impact their ability to perform regular tasks.

Researchers believe that Meltdown and Spectre may be limited to processors manufactured by different companies, but also warn that the design flaws that contribute to Meltdown and Spectre have been present for years. Here are some key details about each flaw:

- **Meltdown**: This flaw can be used to break down the security barriers between a device's applications and operating system in order to access all of the device's data. Meltdown can be used to access desktop, laptop, server and cloud computer systems, and can even be used to steal data from multiple users who share one device. Although researchers have only been able to verify that Meltdown affects processors made by Intel, other processors may also be affected. Many software developers have already released updates that prevent hackers from exploiting Meltdown.

- **Spectre**: This flaw can be used to break down the security barriers between a device's different applications and access sensitive data like passwords, photos and documents, even if those applications adhere to regular security checks. Spectre affects almost every type of computer system, including computers, servers and smartphones. Additionally, researchers have confirmed that the design flaw that enables Spectre is present in Intel, AMD and ARM processors that are used by nearly every computer and mobile device. Software developers are currently working on a patch to prevent the exploitation of Spectre, but some experts believe that future processors may have to be redesigned in order to fix the vulnerability.

When Meltdown and Spectre were originally discovered in 2017, researchers immediately

HIPSKIND SEYFARTH
RISK SOLUTIONS LLC

reported them to major hardware and software companies so work on security fixes could begin without alerting hackers. As a result, services and applications offered by companies like Microsoft, Google, Apple and Amazon have already been updated to help defend against the flaws. However, you shouldn't rely solely on a software patch to protect against these vulnerabilities. Here are some steps you can take to protect your computer systems and devices from Meltdown and Spectre:

- **Update all of your devices immediately, and check for new updates regularly**. You should also encourage your friends, family members and co-workers to do the same.

- **Contact any cloud service providers and third-party vendors you use to ensure that they are protected against Meltdown and Spectre**. Cloud services and computer servers are especially vulnerable to the exploits, as they often host multiple customers on a single device.

- **Install anti-virus and firewall systems to protect against regular malware**. Researchers believe that hackers need to gain access to a device in order to exploit Meltdown or Spectre, so keeping your devices free of malware can help prevent data theft.

For additional risk management updates, contact Hipskind Seyfarth Risk Solutions today.