Subject: **Prevention Against Cyber Espionage - Advisory No 04 February 2018**

1. **Introduction.** Security researchers have discovered kernel level (side-channel) attacks, which affect not only **Intel** but also systems and devices running **AMD, ARM** processors allowing attackers to steal sensitive data from the system memory.

2. **Affected Devices.** Desktop PCs, laptops, tablets, cloud servers and smart phones Intel, AMD, and ARM chips.

3. **Mode of operation**

   a. These hardware vulnerabilities have been categorized into two attacks, named **Meltdown** (CVE-2017-5754) and **Spectre** (CVE-2017-5753 and CVE-2017-5715), which could allow attackers to steal sensitive data which is currently processed on the computer.

   b. Both attacks take advantage of a feature in chips known as "speculative execution," a technique used by most modern CPUs to optimize performance.

   c. Intel processors (x86-64) have a severe hardware-level issue that could allow attackers to access protected kernel memory, which primarily includes information like passwords, login keys, and files cached from disk.

   d. A specialized JavaScript program running in a web browser can recover sensitive kernel-protected data.

4. **Resolution**

   a. **Windows.** Microsoft has issued patch update for Windows 10, while other versions of Windows will be patched on the traditional Patches

   b. **MacOS.** Apple had already fixed most of these security holes in MacOS High Sierra 10.13.2 last month, but MacOS 10.13.3 will enhance or complete these mitigations.

   d. **Linux.** Linux kernel developers have also released patches by implementing kernel page-table isolation (KPTI) to move the kernel into an entirely separate address space.

   e. **Android.** Google has released security patches for Pixel/Nexus users as part of the Android January security patch update. Other users have to wait for their device manufacturers to release a compatible security update.

   f. **Mitigations for Chrome Users.** Since this exploit can be executed through the website, Chrome users can turn on Site Isolation feature on their devices to mitigate these flaws. Here's how to turn Site Isolation on

Windows, Mac, Linux, Chrome OS or Android:-

(1) Copy chrome://flags/#enable-site-per-process and paste it into the URL field at the top of your Chrome web browser, and then hit the Enter key.

(2) Look for Strict Site Isolation, then click the box labeled Enable.

(3) Once done, hit relaunch Now to relaunch your Chrome browser.

5. **Recommendations**

a. Install security patches as discussed at para 4 and apply to all systems including laptops, servers, tablets.

b. Regularly update the system with latest anti-virus.

c. Install and UPDATE well reputed antiviruses such as Kaspersky, Bitdefender, NOD 32, Avast etc.

d. Update all softwares including Windows OS, Internet browser (Mozilla,firefox) and Microsoft office.

e. Don't click on any suspicious website popup during the internet surfing.

f. Don't download attachments from emails unless you are sure about the source.