

Sep 18

1. **Context.** Security researchers have discovered another major **execution flaw**"Foreshadow" in **Intel Core** and **Xeon** lines of processor that may leave users **vulnerable** to **cyber-attacks**. **Foreshadow targets virtual machines** and **SGX** (Software Guards Extensions) in addition to data stored in operating **system's kernel**.

2. **Affected Devices.****Intel, Microsoft, Oracle** and **cloud services** like **Microsoft Azure, Amazon Web Service** and **Google** Compute Engine.

3. **Technical Analysis**

a. **Capabilities of Foreshadow.** **Foreshadow** attacks allow a hacker or malicious application to gain access to the **sensitive data** stored in a **computer's memory** or **third-party clouds** including files, encryption keys, pictures or passwords. Detail as under:-

- (1) Bug attack allow an **unauthorized attacker** to **steal information** residing in protected portion of a **chip's core memory**.
- (2) Flaw targets **virtualization** environments being used by **large cloud** computing providers like **Amazon** and **Microsoft**.
- (3) These **flaws** also disclose **sensitive** information residing in **cache**.
- (4) Foreshadow bug assist a **malicious program** running on the computer to read parts of the **kernel's data** and other programs.

b. **Common Vulnerabilities and Exposure**

- (1) Intel Software Guard Extensions (SGX) — **CVE-2018-3615**.
- (2) Operating systems and System Management Mode (SMM) - **CVE-2018-3620**.
- (3) Virtualization software and Virtual Machine Monitors (VMM) - **CVE-2018-3646**.

4. **Recommendations**

- a. Install **security updates** from **operating system/** virtualization vendors.
- b. It is advised to regularly visit **Company's website** for release of lat t security patches.
- c. Install and **update** well reputed antiviruses such as **Kaspersky, Bitdefender, Nod 32** and **Avast** etc.
- d. **Regularly update** all softwares including **Windows OS, Internet browser (Mozilla, Firefox)** and **Microsoft office**.