PTA CERT for Telecom Sector

Security Advisory-No: Ext:158-21

18, Sep 2018

Threat Classification: Vulnerability

Overview: 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.

Affected Services/Application:

- Intel
- Microsoft
- Oracle
- Cloud services (Microsoft Azure)
- Amazon Web Service
- Google Compute Engine

Technical Analysis:

1) **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.

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

2) **Common Vulnerabilities and Exposure:**

    a) Intel Software Guard Extensions (SGX) - CVE-2018-3615.
    b) Operating systems and System Management Mode (SMM) CVE-2018-3620
    c) Virtualization software and Virtual Machine Monitors (VMM) CVE-2018-3620

Recommendations:

a) Install security updates from operating system/ virtualization vendors.

b) Advised to regularly visit company's website for release of latest security patches.

c) In case of any incident, please report to this office.