GOVERNMENT OF PAKISTAN
CABINET SECRETRIAT,CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB-II)

No. 1-5/2003 (NTISB-II) **Islamabad 11 September, 2018**

Subject: **Advisory — Prevention Against Foreshadow Attacks (Advisory No 158**

C(IT)
Ap
fn/p

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**

14 SEP 2018

M(A)
M(I.T) ✓
A.S (Rev. Div.)

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 latest security patches.

c. Install and **update** well reputed antiviruses such as **Kaspersky, Bitdefender, Nod 32** and **Avast** etc.

As per SOP
for uploading
17.9.2018
Assistant-IT

b. **Update and install latest security patches for OS and all installed applications.**

c. **Install firewall for network security and regularly check logs for any suspicious** communication.

6. **Forwarded for perusal and dissemination of information to all concerned, please.**

Lieutenant Colonel
(Ishtiaq Mahmood Kiani)
Deputy Secretary (NTISB)
Ph# 051-9208854

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments

Copy to :-

SPS to Cabinet Secretary, Cabinet Division , Islamabad

PS to AS-III, Cabinet Division, Islamabad

APS to Secretary, NTISB