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

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

Subject: **Advisory - Prevention Against Foreshadow Attacks (Advisory No 159)**

1. **Context.** Fax communication is .very popular communication medium among **Defense** Organizations, Government **Ministries, regulators, B**ankers, and real estate firms. Security researchers have discovered a vulnerability that can **compromise a** network just by sending a **malicious file** using **Fax.** This unique type of attack is extremely **dangerous** as it only requires **phone number** of target organization

2. **Technical Analysis**

a. Fax machines, if integrated into **all-in-one printers** or connected to a **WI-FI** network / **PSTN phone** line; remote attacker can simply send **a specially crafted image. File** via **fax** to exploit the vulnerabilities and seize control of an enterprise or home network.

b. A **maliciously crafted** file sent to an affected device can cause a **stack** or **static buffer overflow,** which may allow **remote code execution.**

c. The attack involves following buffer overflow vulnerabilities:-

(1) **CVE-2018-5925** - .Triggers while parsing COM markers.
(2) **CVE-2018-5924** - Stack-based issue occurs while parsing DHT markers, which leads to remote code execution.

d. The attacker can use any **exploit** to take over the **connected machines** and further spread the **malicious code** through the network.

3. **Affected Products.** The following models of **Hewlett Packard** (HP) printers are affected to these vulnerabilities:-

a. Page wide Pro.
b. HP Design Jet.
c. HP Office jet.
d. HP DeskJet.
e. HP Envy.

4. **Mitigation Measures.** HP has provided **firmware updates** for impacted printers. To obtain the updated firmware, go to the **HP Software and Drivers page** and find the firmware update from the list of available software.

Recommendations

a. **Strictly follow all mitigation measures mentioned at para 4.**

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

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**

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.

Secy (I.T) / GA&C

17/9/18

DG

This is also should be proper managed record at concerned file as We can also upload on portal to information to all concerned

Sr Manager (NO)/HO

d. **Regularly update** all softwares including **Windows OS, Internet browser (Mozilla, Firefox) and Microsoft office.**

5. 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