

**GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT, 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, Bankers, 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.

5. **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