PTA CERT for Telecom Sector

Security Advisory-No: Ext:159-22

19, Sep 2018

Threat Classification: Vulnerability

Overview: 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.

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.

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

- Page wide Pro
- HP Design Jet
- HP Office Jet
- HP Desk Jet
- HP Envy

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 above.

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