Subject: **Advisory Prevention Against Cyber Espionage (Advisory No 23) Apr 18**

1. **Introduction.** A hacking group named **`JHT'** hijacked a significant number of Ciscodevices belonging to organizations in **Russia/ Iran** and left a message that reads "Do not mess with our elections" with an American flag. This campaign impacted approximately 3,500 network switches in Iran though a majority of them were already restored.

2. **Technical Analysis**

   a. The attack involves recently disclosed remote code execution vulnerability **(CVE-2018-0171)** in Cisco Smart Install Client that could allow attackers to take full control of the network equipment.

   b. The Cisco Smart Install protocol can be abused to modify the TFTP server setting, exfiltrate configuration files via TFTP, modify the configuration file, replace the 105 image and setup accounts allowing for the execution of IOS commands.

   c. According to the scanning engine Shodan, more than 165,000 systems are still exposed on the Internet.

3. **Affected Products.** Catalyst 4500 Supervisor Engines, Cisco Catalyst 3850 Series Switches and Cisco Catalyst 2960 Series Switches devices, as well as all devices that fall into the Smart Install Client type are potentially vulnerable.

4. **Recommendations.**

   a. Administrators who have install the Cisco Smart Install feature, should disable it entirely with the configuration command — "no vstack".

   b. Network administrators are highly recommended to install patches to address this vulnerability (CVE-2018-0171).