PTA CERT for Telecom Sector

Security Advisory-No: 26

30th, Oct 2018

Threat Classification: Vulnerability

Name:

- Command Injection Vulnerability (CVE-2018-3953, CVE-2018-3954, CVE-2018-3955)

Source: Affect following products of Linksys:

- Linksys E Series Line of routers

Distribution: The vulnerabilities can be exploited in the following versions of Linksys products:

a) Linksys E1200 Firmware Version 2.0.09
b) Linksys E2500 Firmware Version 3.0.04

Exploited Vulnerabilities: Attackers can exploit above vulnerabilities by sending an authenticated HTTP request to the device, on successful exploitation, the attackers could allow executing arbitrary code on the affected device that enables the attackers to gain control of the affected device to perform malicious activities such as the unauthorized installation of malicious codes.

Recommendations:

a) Device Administrator must updates firmware of the affected devices to the latest release from following links.
   - https://www.linksys.com/us/support-article?articleNum=148523
   - https://www.linksys.com/us/support-article?articleNum=148377

b) Designate a PoC for your network users for seeking assistance and reporting security issues.

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