PTA Security Advisory-No: 46

03, April 2019

Threat Classification: Security Vulnerability

Name of Vulnerability:

Denial of Service Vulnerability:

CVE-2019-1737, CVE-2019-1738, CVE-2019-1739, CVE-2019-1740, CVE-2019-1741, CVE-2019-1746
CVE-2019-1747, CVE-2019-1750, CVE-2019-1751, CVE-2019-1752, CVE-2019-1760

Elevation of Privilege Vulnerability:

CVE-2019-1753, CVE-2019-1754

Security Restriction Bypass Vulnerability:

CVE-2019-1758, CVE-2019-1759

Information Disclosure Vulnerability:

CVE-2019-1742, CVE-2019-1761, CVE-2019-1762, CVE-2019-1745, CVE-2019-1755, CVE-2019-1756

Arbitrary File Upload Vulnerability:

CVE-2019-1743

Improper Service Validation Vulnerability:

CVE-2019-1748
CVE-2019-1757

Source: Affect following products of Cisco

- Cisco IOS
- Cisco IOS XE

Exploited Vulnerabilities: Multiple vulnerabilities were identified in Cisco products, a remote attacker could exploit some of these vulnerabilities to trigger denial of service condition, elevation of privilege, remote code execution, disclose sensitive information and bypass security restriction on the targeted system.

Recommendations:

1) Update following official patches/commands/products to fix the aforementioned vulnerabilities:
   - https://tools.cisco.com/security/center/publicationListing.x
2) Whenever required, run software with minimal access rights and privileges.
3) Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
4) Use only licensed software and avoid to use/ download cracked or pirated software.

5) Designate PoC from your security / network team (if yet not designated), for seeking assistance and reporting security issues.

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