PTA Security Advisory-No: 47

05 April 2019

Threat Classification: Security Vulnerability

Name: Signature verification bypass vulnerability (CVE-2019-5300)

Source: Affect following products of Huawei:

- Huawei Enterprise Router / Firewall

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

Product Name	Affected Version	Updated Version to Fix Vulnerability
Huawei AR1200 Series Huawei AR1200-S Series Huawei AR150 Series Huawei AR160 Series Huawei AR2200 Series Huawei AR2200 Series Huawei AR2200-S Series Huawei AR3200 Series Huawei SRG1300 Series Huawei SRG2300 Series Huawei SRG3300 Series	V200R007C00 V200R008C20 V200R008C50 V200R009C00 V200R010C00 V200R008C20 V200R008C50 V200R009C00 V200R010C00	V200R010SPH003

Exploited Vulnerabilities: Hackers with high privileges may exploit the vulnerability exists in Huawei products to bypass integrity checks for software images and install a malicious software image on the affected device. On the successfully exploit, the attacker could bypass integrity checks for software images and install the malicious software images on the affected device.

Recommendations:

- Update following official firmware/image to fix the aforementioned vulnerabilities:
  - https://support.huawei.com/enterprise/en/software/index.html
- Whenever required, run software with minimal access rights and privileges.
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoids download/use of crack and pirated software.
- Designate PoC from your security / network team (if yet not designated), for seeking assistance and reporting security issues.
- In case of any incident, please report to this office.