PTA Security Advisory-No: 49

02 May 2019

Threat Classification: Backdoors in Huawei MateBook (Laptop) Driver/Software

Name:

- Privilege escalation vulnerability (CVE-2019-5241)
- Arbitrary code execution vulnerability (CVE-2019-5242)

Source: Affect following products of Huawei:

- Huawei PCManager

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

Product Name	Affected Version	Resolved Product and Version
PCManager	PCManager 9.0.1.66 and Prior	PCManager 9.0.1.80 and later

Exploited Vulnerabilities: Hackers may exploit the following vulnerability exists in Huawei PCManager Product.

CVE-2019-5241:

Privilege escalation vulnerability exists in Huawei PCManager could allow the remote attackers to gain high privileges in the system. The attacker can trick the victim to install and run a malicious application.

CVE-2019-5242:

Arbitrary code execution vulnerability exists in Huawei PCManager could allow the remote attackers to execute arbitrary code on the system and read/write memory information. The attacker can trick the victim to install and run a malicious application.

Recommendations:

- Update following official firmware/image to fix the aforementioned vulnerabilities:
  - https://consumer.huawei.com/en/support/laptops/matebook-13/
- 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.