PTA Cyber Security Advisory No:083   **28-May-2020**

Name: HUAWEI CloudEngine Product Denial of Service (DoS) Vulnerability
          (CVE-2020-1870)

Threat Classification: Denial of Service

Affected Systems: Affects the following Huawei CloudEngine product versions:

- **CloudEngine 12800**: V200R019C00, V200R019C00SPC600, V200R019C00SPC800, V200R019C10
- **CloudEngine 6800**: V200R019C00SPC800

Summary:

A Denial of Service (DOS) vulnerability exists in the above mentioned Huawei products due to improper memory management or memory leakage. Attacker can perform a series of operations to exploit this vulnerability and successful exploit may cause a denial of service condition on the affected system.

Severity	HIGH
Attack Vector	Network
Privileges required	None

For further details, please visit following official link:

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200527-01-dos-en

Recommendations:

- Software updates of Huawei products are available at following official link:
  https://support.huawei.com/enterprise/en/software/index.html

- As per vendor recommendation, please visit the section "Obtaining Fixed Software" at following official link for the remediation process of the aforementioned vulnerability:
  https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200527-01-dos-en

- In all cases, ensure the availability of stable version, before upgrade, by the relevant vendor.

- In all cases, also ensure that devices to be upgraded to new release meet the requirements set by the vendor.

- Whenever required, access the system 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 avoid download/use of cracked and pirated software.

- Designate a 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.