Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No:088 **28-June-2020**

Name: HUAWEI OceanStor 9000 FasterXML Jackson-databind Injection Vulnerability (CVE-2020-8840)

Threat Classification: Remote Code Execution

Affected Systems: Affects the following Huawei OceanStor 9000 product versions:

- V300R006C20
- V300R006C20SPC100
- V300R006C20SPC200
- V300R006C20SPC300

Resolved Product with version: OceanStor 9000 V5 7.1.1

Summary:

A Java library, jackson-databind could de-serialize the data without proper validation which could allow a malicious client to perform remote code execution on a service with the required characteristics.

Severity	**CRITICAL**
Attack Vector	Network
Privileges required	None

For further details, please visit following official link:

https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200610-01-fastjason-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-20200610-01-fastjason-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.