Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No:081 **11-May-2020**

Name: Huawei AR3200 Routers Improper Authentication Vulnerability (CVE-2020-9068)

Threat Classification: Privilege Escalation

Affected Systems: Affects the following Huawei AR3200 product versions:

- V200R007C00SPC900
- V200R007C00SPCa00
- V200R007C00SPCb00
- V200R007C00SPCc00
- V200R009C00SPC500

Summary:

This vulnerability can be exploited only when the malicious actor can access the network where the affected device is present. Successful exploit of this vulnerability may allow the attacker certain permissions on the affected device.

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-20200422-01-authentication-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 aforementioned vulnerability: https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200422-01-authentication-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.