Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:108 **19-10-2020**

Name: IBM QRadar SIEM vulnerable to untrusted data Deserialization (CVE-2020-4280)

Threat Classification: Code Execution

Affected Products:

- IBM QRadar SIEM 7.4.0 - 7.4.1 GA
- IBM QRadar SIEM 7.3.0 - 7.3.3 Patch 4

Summary:

A vulnerability due to insecure deserialization of user-supplied content could allow an attacker to execute arbitrary commands on the IBM QRadar system. By sending a malicious serialized Java object, an attacker could exploit this vulnerability.

Attack Severity	**HIGH**
Attack Vector	Network
Privileges required	Low

For more information, please find below official link:
https://www.ibm.com/support/pages/node/6344079

Recommendations:

- Please visit the '**Remediation/Fixes**' section of the below mentioned official link for the remediation of the aforementioned vulnerability:
  https://www.ibm.com/support/pages/node/6344079

- To get the latest notifications and stay informed of the Security updates of critical IBM software, please visit following official link:
  https://www.ibm.com/support/pages/node/718119

- 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, 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 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.