Advisory Alert

Alert Number: AAA20220919 **Date:** September 19, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**	Denial of Service Vulnerabilities

Description

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	**Denial of Service Vulnerabilities** (CVE-2020-29651, CVE-2020-28493)
Description	IBM has released security updates addressing multiple Denial of service vulnerabilities that exists in the third party libraries that used by the IBM QRadar Network Threat Analytics product. **CVE-2020-29651** – This vulnerability exists due to a regular expression in the svnwc.py component used in the Python Py package that used in the QRadar Network Threat Analytics. Using this vulnerability a remote attacker can cause compute-time denial of service by supplying malicious input to the blame functionality. **CVE-2020-28493** – This vulnerability exists due to a flaw in the email regex in the Pallets jinja2, a third-party component that used by the IBM QRadar Network Threat Analytics. Using this vulnerability a remote attacker can cause a denial of service condition by sending a specially-crafted input IBM highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Security QRadar Network Threat Analytics version 1.0.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6618759 https://www.ibm.com/support/pages/node/6618757

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.