Advisory Alert

Alert Number: AAA20241226 **Date:** December 26, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45296, CVE-2024-8986, CVE-2024-21489)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Security QRadar Log Management AQL Plugin. **CVE-2024-45296** - pillarjs Path-to-RegExp is vulnerable to a denial of service, caused by a regular expression denial of service (ReDoS) flaw. By sending a specially crafted regex request, a remote attacker could exploit this vulnerability to cause a denial of service condition. **CVE-2024-8986** - grafana-plugin-sdk-go could allow a remote attacker to obtain sensitive information, caused by insufficiently protected credentials. By sending a specially crafted request, an attacker could exploit this vulnerability to obtain sensitive information. **CVE-2024-21489** - uPlot could allow a remote attacker to execute arbitrary code on the system, caused by a prototype pollution flaw in the uplot.assign function. By adding or modifying properties of Object.prototype using a __proto__ or constructor payload, an attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security QRadar Log Management AQL Plugin versions 1.0 - 1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7179757

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.