Advisory Alert

Alert Number: AAA20240202 **Date:** February 2, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-38900, CVE-2023-45857, CVE-2022-25883, CVE-2022-25927)
Description	IBM has released security updates addressing Multiple Vulnerabilities that exist in IBM QRadar Assistant App for IBM QRadar SIEM. **CVE-2022-38900 -** A denial of service vulnerability exists in Decode-uri-component, caused by improper input validation by the decode Component's function. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause the application to crash. **CVE-2023-45857** - A cross-site request forgery vulnerability exists in Axios, caused by improper validation of user-supplied input. By inserting the X-XSRF-TOKEN header using the secret XSRF-TOKEN cookie value in all requests to any server when the XSRF-TOKEN0 cookie is available, and with the Credentials setting turned on, an attacker could exploit this vulnerability to perform cross-site scripting attacks, Web cache poisoning, and other malicious activities. **CVE-2022-25883** - A denial of service vulnerability exists in Node.js semver package, caused by a regular expression denial of service (ReDoS) flaw in the new Range function. By providing specially crafted regex input, a remote attacker could exploit this vulnerability to cause a denial of service. **CVE-2022-25927** - A denial of service vulnerability exists in Node.js ua-parser-js module, caused by a regular expression denial of service (ReDoS) flaw. By sending specially-crafted regex input, a remote attacker could exploit this vulnerability to cause a denial of service. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
.Affected Products	IBM QRadar Assistant Version 1.0.0 - 3.6.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7114134

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.