Advisory Alert

Alert Number: AAA20230607 **Date:** June 7, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**, **Medium**	Multiple vulnerabilities
Apache Guacamole	**Medium**	Multiple vulnerabilities

Description

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-25881, CVE-2021-23440, CVE-2022-24785, CVE-2022-46175)
Description	IBM has released security update addressing multiple vulnerabilities that exist in their IBM QRadar Deployment Intelligence App. Successful exploitation of these vulnerabilities could lead to denial of service , path traversal and arbitrary code execution. **CVE-2022-25881-** Denial of service vulnerability due to regular expression denial of service (ReDoS) flaw in Node.js http-cache-semantics module.A remote attacker could exploit this vulnerability by sending a specially-crafted regex input using request header values. **CVE-2021-23440-** Arbitrary code execution vulnerability due to prototype pollution flaw in Nodejs set-value module.An attacker could exploit this vulnerability by adding or modifying properties of Object.prototype using a __proto__ or constructor payload. **CVE-2022-24785-** Path traversal vulnerability due to improper validation of user supplied input in Moment.js .A remote attacker could exploit this vulnerability by sending a specially-crafted locale string containing "dot dot" sequences (/../) to switch arbitrary moment locale. **CVE-2022-46175 -** Arbitrary code execution vulnerability due to prototype pollution flaw in the JSON5. remote authenticated attacker could exploit this vulnerability by adding or modifying properties of Object.prototype using a __proto__ or constructor payload. IBM recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	IBM QRadar Deployment Intelligence App 2.0.0 - 3.0.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7001723

Affected Product	**Apache Guacamole**
Severity	**Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-30575,CVE-2023-30576)
Description	Apache Guacamole has released security update addressing multiple vulnerabilities. Successful exploitation of these vulnerabilities could lead to Use-after-free condition and code injection. **CVE-2023-30575-** Code injection vulnerability in Apache Guacamole 1.5.1 and older.During Guacamole protocol handshake,attacker could inject Guacamole instructions through specially-crafted data. **CVE-2023-30576-** Apache Guacamole 0.9.10 through 1.5.1 may continue to reference a freed RDP audio input buffer. Depending on timing, this may allow an attacker to execute arbitrary code with the privileges of the guacd process. Apache Guacamole recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Apache Guacamole 1.5.1 and older
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://guacamole.apache.org/security/

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.