July 10, 2023

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of IBM Security Patch Day saw the release of over 95 new Patch Day Security Notes. The vulnerability affects versions detailed in the table below.

CVE / Description / Product	Risk	CVSS
Multiple Vunerabilities in IBM Java SDK affect IBM Cloud Pak System **Product - IBM Cloud Pak System Software**	**CRITICAL**	**9.8**
Vulnerability in Golang Go affects IBM Cloud Pak System [CVE-2023-24538] **Product – IBM Cloud Pak System Software**	CRITICAL	9.8
IBM QRadar SIEM includes components with known vulnerabilities **Product – IBM Security QRadar SIEM**	**CRITICAL**	**9.8**
Vulnerabilities have been identified in OpenSSL, Apache HTTP Server and other system libraries shipped with the DS8000 Hardware Management Console (HMC) **Product – DS8900F**	**CRITICAL**	**9.8**
Vulnerabilities have been identified in OpenSSL, Apache HTTP Server and other system libraries shipped with the DS8000 Hardware Management Console (HMC) **Product – DS8900F**	**High**	**9.0**
IBM QRadar SIEM includes components with known vulnerabilities.	**CRITICAL**	**9.8**

Product – IBM Cloud Automation Manager		
A security vulnerability in Node.js netmask module affects IBM Cloud Automation Manager **Product – IBM Cloud Automation Manager**	**CRITICAL**	9.1
A security vulnerability in Node.js jison affectsI BM Cloud Automation Manager **Product – IBM Security QRadar SIEM**	**CRITICAL**	**9.8**
A security vulnerability in Node.js node-forge module affects IBM Cloud Automation Manager. **Product – IBM Cloud Automation Manager**	CRITICAL	9.8
IBM QRadar SIEM includes components with known vulnerabilities **Product – IBM Security QRadar SIEM**	CRITICAL	9.8
IBM Watson Assistant for IBM Cloud Pak for Data is vulnerable to multiple vulerabilities in TensorFlow **Product – IBM Watson Developer Cloud**	CRITICAL	9.8
IBM Watson Assistant for IBM Cloud Pak for Data is vulnerable to VMware Tanzu Spring Framework security bypass and denial of service vulnerabilities [CVE-2023-20860, CVE-2023-20861] **Product – IBM Watson Developer Cloud**	**CRITICAL**	**9.8**
IBM Cloud Pak for Network Automation 2.4.5 addresses multiple security vulnerabilities **Product – IBM Cloud Pak for Network Automation**	**CRITICAL**	**9.8**
IBM Cloud Pak for Network Automation 2.4.6 fixes multiple security vulnerabilities **Product – IBM Cloud Pak for Network Automation**	**CRITICAL**	**9.8**
IBM WebSphere Application Server Liberty is vulnerable to server-side request forgery due to Apache CXF (CVE-2022-46364) **Product – WebSphere Application Server**	**CRITICAL**	**9.8**

Multiple Vulnerabilities in Multicloud Management Security Services **IBM Cloud Pak for Multicloud Management**	CRITICAL	9.8
Multiple Vulnerabilities in Multicloud Management Security Services **IBM Cloud Pak for Multicloud Management**	CRITICAL	9.8
Multiple Vulnerabilities in Multicloud Management Security Services **IBM Cloud Pak for Multicloud Management**	CRITICAL	9.8
Multiple Security Vulnerabilities have been fixed in IBM Security Verify Access **IBM Security Verify Access**	CRITICAL	9.8
IBM MQ is affected by vulnerabilities in libcURL (CVE-2023-23916, CVE-2023-27535) **IBM MQ**	CRITICAL	9.8
IBM Cloud Pak for Network Automation v2.4.3 addresses multiple security vulnerabilities **IBM Cloud Pak for Network Automation**	CRITICAL	9.8
A security vulnerability in Node.js affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in Node.js affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in Node.js ini module affects IBM Cloud Automation Manager. **IBM Cloud Automation Manager**	CRITICAL	9.8
IBM Cloud Automation Manager is affected by an issue with Docker 19.03.x before 19.03.1. **IBM Cloud Automation Manager**	CRITICAL	9.8

A Security Vulnerability affects IBM Cloud Automation Manager - Go (CVE-2019-17596) **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in Node.js affects IBM Cloud Automation Manager. **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in GO affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in GO affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in Node.js nconf affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in Node.js marked module affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in Node.js node-forge affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in Node.js node-forge affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in GO affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in golang affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8

A security vulnerability in golang affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in Node.js marked module affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in log4j v1.2 affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in GO affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in Node.js pac-resolver module affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in Node.js jsonpointer module affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in Node.js xmlhttprequest-ssl module affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in NGINX ffects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in Node.js affects IBM Cloud Automation Manager **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in Node.js Lodash module affects IBM Cloud Automation Manager. **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in GO affects IBM Cloud Automation Manager.	CRITICAL	9.8

IBM Cloud Automation Manager		
A security vulnerability in Node.js y18n module affects IBM Cloud Automation Manager. **IBM Cloud Automation Manager**	CRITICAL	9.8
A security vulnerability in GO affects IBM Cloud Automation Manager. **IBM Cloud Automation Manager**	CRITICAL	9.8
IBM Cloud Pak for Network Automation v2.4.3 addresses multiple security vulnerabilities **IBM Cloud Pak for Network Automation**	CRITICAL	9.8

Exploitability Metrics
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: Required

This vulnerability is rated as a Critical risk. A software patch exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-21930 CVE-2023-2597 CVE-2022-0778 CVE-2021-23840 CVE-2020-27221 CVE-2020-14583 CVE-2020-14593 CVE-2023-30445 CVE-2023-30431 CVE-2023-27558 CVE-2023-24538 CVE-2023-21930 CVE-2022-43680 CVE-2022-34917 CVE-2022-37434 CVE-2022-37734 CVE-2021-43138 CVE-2018-20060
- Overview - Security Bulletins - IBM Support