Advisory Alert

Alert Number: AAA20220602 **Date:** June 2, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Remote Code Execution Vulnerability
IBM	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	Cisco
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2022-22965)
Description	Cisco has found a flaw which leads spring MVC or Spring WebFlux application running on JDK 9+ vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. It is not vulnerable when the application is deployed as a Spring Boot executable jar, i.e. the default Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco CX Cloud Agent Software 2.0 Cisco Automated Subsea Tuning 2.1.0 Cisco Crosswork Network Controller 3.0.2 , 2.0.2 Cisco Crosswork Optimization Engine 3.1.1, 2.1.1 Cisco Crosswork Zero Touch Provisioning (ZTP) 3.0.2, 2.0.2 Cisco DNA Center 2.3.3.3, 2.2.3.6, 2.2.2.9 Cisco Evolved Programmable Network Manager 6.0.1.1, 5.1.4.1, 5.0.2.3 Cisco Managed Services Accelerator (MSX) 4.2.3 Cisco Optical Network Planner 4.2, 5.0 Cisco WAN Automation Engine (WAE) Live 7.5.2.1, 7.4.0.2, 7.3.0.3 Cisco WAN Automation Engine (WAE) 7.5.2.1, 7.4.0.2, 7.3.0.3 Data Center Network Manager (DCNM) 11.5.4 Nexus Dashboard Fabric Controller (NDFC) 12.1.1 Cisco Optical Network Controller 2.0 Cisco Software-Defined AVC (SD-AVC) 4.3.1, 4.4.0 Cisco Enterprise Chat and Email 12, 12.5, 12.6 ES2 Cisco Meeting Server 3.5.0, 3.4.2, 3.3.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-java-spring-rce-Zx9GUc67

Affected Product	IBM
Severity	**High**, **Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-35550 , CVE-2021-2341 , CVE-2021-35603, CVE-2022-24785)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of the most severe vulnerabilities could cause cross-site scripting, denial of service, sensitive data exposure and directory traversal vulnerability. IBM highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	IBM Db2 Mirror for i 7.5, 7.4 IBM Db2 V9.7, V10.1, V10.5, V11.1 and V11.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/blogs/psirt/security-bulletin-ibm-db2-mirror-for-i-is-vulnerable-to-denial-of-service-due-to-gson-217225-2/ https://www.ibm.com/blogs/psirt/security-bulletin-ibm-db2-mirror-for-i-is-vulnerable-to-cross-site-scripting-due-to-angular-220414/ https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilities-in-java-se-that-could-allow-an-unauthenticated-attacker-to-obtain-sensitive-information-affect-ibm-db2-cve-2021-35603-cve-2021-35550-cve-202/

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.