Advisory Alert

Alert Number: AAA20220523 **Date:** May 23, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Arbitrary code execution vulnerability
IBM	**Medium**	Spoofing vulnerability
Cisco	**Medium**	Open port vulnerability

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Arbitrary code execution vulnerability (CVE-2021-23450)
Description	IBM has released security updates addressing arbitrary code execution vulnerability that exists in WebSphere Application Server Liberty. Dojo could allow a remote attacker to execute arbitrary code on the system, caused by a prototype pollution in the setObject function. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM strongly recommends to apply the available patch updates at earliest to avoid issues.
Affected Products	IBM TXSeries for Multiplatforms version 9.1, 8.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6588149

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Spoofing vulnerability (CVE-2022-22365)
Description	IBM has released security updates for IBM WebSphere Application Server, with the Ajax Proxy Web Application (AjaxProxy.war) deployed, which is vulnerable to spoofing by allowing a man-in-the-middle attacker to spoof SSL server hostnames. IBM recommends to apply necessary security fixes to avoid issues
Affected Products	IBM WebSphere Application Server version 9.0, 8.5, 8.0, 7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6587947

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Open port vulnerability (CVE-2022-20821)
Description	Cisco has released security updates addressing a vulnerability in the health check RPM of Cisco IOS XR Software which could allow an unauthenticated, remote attacker to access the Redis instance that is running within the NOSi container. Cisco recommends to apply necessary security fixes at earliest to avoid issue
Affected Products	Cisco 8000 Series Routers running a vulnerable release of Cisco IOS XR Software with the health check RPM installed and active.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-redis-ABJyE5xK

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.