TLP: WHITE

Advisory Alert

Alert Number: **AAA20230706** **Date:** **July 6, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**	Security restrictions bypass

Description

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20178, CVE-2023-20185, CVE-2023-20133, CVE-2023-20180, CVE-2023-20207, CVE-2023-20210)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause Privilege Escalation, Information Disclosure, Web UI Vulnerabilities. Cisco recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Cisco AnyConnect Secure Mobility Client for Windows Software 4.10 and earlier Cisco Secure Client for Windows Software 5.0 Cisco Nexus 9000 Series Fabric Switches 14.0 and later Cisco Webex Meetings Cisco Duo Authentication Proxy Release 5.8.0, 6.0.0 BroadWorks Application Delivery Platform, Database Troubleshooting Server, Media Server, and Service Control Function Server Cisco BroadWorks Application Server 22.0 and earlier,23.0, 24.0 BroadWorks Database Server, Execution Server, Network Database Server, and Network Function Manager 22.0 and earlier BroadWorks Network Server, Profile Server, and Xtended Services Platform 22.0 and earlier, 23.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Security restrictions bypass (CVE-2023-35890)
Description	IBM has released security updates addressing Security restrictions bypass vulnerability that exist in IBM WebSphere Application Server. This vulnerability could cause improper encoding in a local configuration file and the attacker can bypass expected security IBM recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	IBM WebSphere Application Server 9.0 IBM WebSphere Application Server 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7007857

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.