Advisory Alert

Alert Number: AAA20220908 **Date:** September 8, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**, **Medium**	Multiple Vulnerabilities
IBM	**Medium**	HTTP header injection vulnerability

Description

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20863, CVE-2022-20696 CVE-2022-28199, CVE-2022-20923)
Description	Cisco has released Security Updates addressing multiple vulnerabilities that exist in their products. **CVE-2022-20863**- A vulnerability exists in the Cisco Webex App, formerly Webex Teams, due to the improper handling of character render. An attacker could exploit this vulnerability by sending messages within the application interface. A successful exploit could allow the attacker to modify the display of links or other content within the interface, potentially allowing the attacker to conduct phishing or spoofing attacks. **CVE-2022-20696**- A vulnerability exists in the binding configuration of Cisco SD-WAN vManage Software due to the insufficient protection mechanisms on the affected system's messaging server container ports. To exploit this vulnerability, the attacker must be able to send network traffic to interfaces within the VPN0 logical network. An attacker could view and inject messages into the messaging service, which can cause configuration changes or cause the system to reload. **CVE-2022-28199**- A vulnerability exists in the NVIDIA Data Plane Development Kit (MLNX_DPDK) due to improper error handling. A remote attacker could cause a denial of service and some impact on data integrity and confidentiality. **CVE-2022-20923**- A vulnerability exists in the IPSec VPN Server authentication functionality of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers due to the improper implementation of the password validation algorithm. An attacker could bypass authentication and access the IPSec VPN network with crafted credentials. The attacker may obtain privileges that are the same level as an administrative user, depending on the crafted credentials that are used. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco Webex App Earlier than 42.7 Cisco SD-WAN vManage Earlier than 20.3 Cisco SD-WAN vManage 20.3, 20.6, 20.7, 20.8 and 20.9 RV110W Wireless-N VPN Firewall RV130 VPN Router RV130W Wireless-N Multifunction VPN Router RV215W Wireless-N VPN Router Cisco Catalyst 8000V Edge Software 17.6, 17.7 and 17.8 Adaptive Security Virtual Appliance (ASAv) 9.17 and 9.18 Secure Firewall Threat Defense Virtual (formerly FTDv) 7.1 and 7.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-app-qrtO6YC2 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-msg-serv-AqTup7vs https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mlx5-jbPCrqD8 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-rv-vpnbypass-Cpheup9O

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	HTTP header injection vulnerability (CVE-2022-34165)
Description	IBM has released Security Updates addressing an HTTP header injection vulnerability in IBM WebSphere Application Server and IBM WebSphere Application Server Liberty. The vulnerability exists due to improper validation. An attacker could conduct various attacks against the vulnerable system, including cache poisoning and cross-site scripting. IBM highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	IBM WebSphere Application Server Liberty 17.0.0.3 - 22.0.0.9 IBM WebSphere Application Server 9.0 IBM WebSphere Application Server 8.5 IBM WebSphere Application Server 8.0 IBM WebSphere Application Server 7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6618747

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.