Advisory Alert

Alert Number: AAA20220804 **Date:** August 4, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities
RedHat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20827, CVE-2022-20841, CVE-2022-20842)
Description	Cisco has released a security update addressing multiple critical vulnerabilities that exist in their Cisco Small Business RV Series Routers. These vulnerabilities could allow an unauthorized, remote attacker to run arbitrary code or cause a denial of service (DoS) condition on a vulnerable device. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	RV160 VPN Routers RV160W Wireless-AC VPN Routers RV260 VPN Routers RV260P VPN Routers with PoE RV260W Wireless-AC VPN Routers RV340 Dual WAN Gigabit VPN Routers RV340W Dual WAN Gigabit Wireless-AC VPN Routers RV345 Dual WAN Gigabit VPN Routers RV345P Dual WAN Gigabit POE VPN Routers
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20820, CVE-2022-20852, CVE-2022-20914, CVE-2022-20816, CVE-2022-20869)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could cause cross-site scripting (XSS), sensitive information disclosure, frame hijacking and arbitrary file execution. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Web interface of Cisco Webex Meetings Cisco ISE Software 2.3 and earlier Cisco ISE Software 2.4, 2.6, 2.7, 3.0, 31 Cisco Unified CM and Cisco Unified CM SME 11.5, 12.5, 14 Cisco BroadWorks Call Center 22.0, 23.0, 24.0 Cisco BroadWorks Receptionis 22.0, 23.0, 24.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-xss-frmhijck-kO3wmkuS#vp https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-pwd-WH64AhQF https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-file-delete-N2VPmOnE https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-xss-xbhfr4cD

Affected Product	**RedHat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-44906, CVE-2022-24823, CVE-2022-25647)
Description	RedHat has released security updates to address multiple vulnerabilities that exist in JBoss Enterprise Application. Successful exploitation of these vulnerabilities could cause deserialization of untrusted data, prototype pollution and sensitive data exposure. RedHat highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	JBoss Enterprise Application Platform 7.4 for RHEL 7 x86_6 JBoss Enterprise Application Platform 7.4 for RHEL 9 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:5892 https://access.redhat.com/errata/RHSA-2022:5894

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.