Advisory Alert

Alert Number: AAA20220203 **Date:** February 3, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	Multiple vulnerabilities

Description

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-20699, CVE-2022-20700, CVE-2022-20701, CVE-2022-20702, CVE-2022-20703, CVE-2022-20704, CVE-2022-20705, CVE-2022-20706, CVE-2022-20707, CVE-2022-20708, CVE-2022-20709, CVE-2022-20710, CVE-2022-20711, CVE-2022-20712, CVE-2022-20749)
Description	Cisco has released updates addressing multiple vulnerabilities that exists in their products such as Remote Code Execution, Privilege Escalation, Digital Signature Verification Bypass Vulnerability, SSL Certificate Validation Vulnerability, Improper Session Management Vulnerability, Command Injection Vulnerabilities, Arbitrary File Upload Vulnerability, Denial of Service, Arbitrary File Overwrite Vulnerability. Cisco highly recommends to apply necessary security fixes 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-smb-mult-vuln-KA9PK6D

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.