Severity

Medium

Analysis Summary

CVE-2022-20753 CVSS:4.7

Cisco Small Business RV Series Routers could allow a remote authenticated attacker to execute arbitrary code on the system, caused by improper validation of user-supplied input. By sending specially-crafted input to a specific field in the web-based management interface, an attacker could exploit this vulnerability to execute arbitrary code on the system.

CVE-2022-20734 CVSS:4.4

Cisco SD-WAN vManage Software could allow a local authenticated attacker to obtain sensitive information, caused by insufficient file system restrictions. By accessing the vshell, an attacker could exploit this vulnerability to obtain sensitive information

CVE-2022-20801 CVSS:4.7

Cisco Small Business RV Series Routers could allow a remote authenticated attacker to execute arbitrary commands on the system, caused by improper validation of user-supplied input. By sending a specially-crafted input to a specific field in the web-based management interface, an attacker could exploit this vulnerability to execute arbitrary commands on the system.

CVE-2022-20764 CVSS:6.5

Cisco TelePresence Collaboration Endpoint and RoomOS Software is vulnerable to a denial of service, caused by insufficient validation of URIs in web engine feature. By using debug URIs in the web engine, a remote authenticated attacker could exploit this vulnerability to simulate a process crash.

CVE-2022-20794 CVSS:4.4

Cisco TelePresence Collaboration Endpoint and RoomOS Software could allow a remote attacker to conduct phishing attacks, caused by insufficient input validation in the web engine. An attacker could exploit this vulnerability using a specially-crafted URL to redirect users to an attacker-controlled destination.

CVE-2022-20799 CVSS:4.7

Cisco Small Business RV Series Routers could allow a remote authenticated attacker to execute arbitrary commands on the system, caused by improper validation of user-supplied input. By sending a specially-crafted input to a specific field in the web-based management interface, an attacker could exploit this vulnerability to execute arbitrary commands on the system.

Impact

- Code Execution
- Information Disclosure
- Command Execution
- Denial of Service

Indicators Of Compromise

CVE

- CVE-2022-20753
- CVE-2022-20734
- CVE-2022-20801
- CVE-2022-20764

- CVE-2022-20794
- CVE-2022-20799

Affected Vendors

- Cisco

Affected Products

- Cisco RV345 Dual WAN Gigabit VPN Routers
- Cisco RV340W Dual WAN Gigabit Wireless-AC VPN Router
- Cisco RV340 Dual WAN Gigabit VPN Router
- Cisco RV345P Dual WAN Gigabit POE VPN Router
- Cisco SD-WAN vManage software
- Cisco RoomOS Software
- Cisco Telepresence CE Software

Remediation

Refer to Cisco Security Advisory for patch, upgrade, or suggested workaround information.

CVE-2022-20753 CVE-2022-20734 CVE-2022-20801 CVE-2022-20764 CVE-2022-20794 CVE-2022-20799