Severity

Medium

Analysis Summary

CVE-2022-20786 CVSS:5.4

Cisco Unified Communications Manager IM and Presence Service is vulnerable to SQL injection. A remote authenticated attacker could send specially-crafted SQL statements using user-submitted parameters, which could allow the attacker to view, add, modify or delete information in the back-end database.

CVE-2022-20787 CVSS:5.7

Cisco Unified Communications Manager and Cisco Unified CM Session Management Edition are vulnerable to cross-site request forgery, caused by improper validation of user-supplied input. By persuading an authenticated user to visit a malicious Web site, a remote authenticated attacker could send a malformed HTTP request to perform unauthorized actions. An attacker could exploit this vulnerability to perform cross-site scripting attacks, Web cache poisoning, and other malicious activities.

CVE-2022-20778 CVSS:6.1

Cisco Webex Meetings is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the web-based interface of the authentication component. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

CVE-2022-20788 CVSS:6.1

Cisco Unified Communications Manager (Unified CM), Cisco Unified CM Session Management Edition (Unified CM SME), and Cisco Unity Connection are vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the web-based management interface. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

CVE-2022-20732 CVSS:7.8

Cisco Virtualized Infrastructure Manager could allow a local authenticated attacker to gain elevated privileges on the system, caused by improper access permissions for certain configuration files. By reading the affected configuration files, an authenticated attacker could exploit this vulnerability to access to the database to elevate privileges on the affected device.

CVE-2022-20783 CVSS:7.5

Cisco TelePresence Collaboration Endpoint and RoomOS Software are vulnerable to a denial of service, caused by improper input validation. By sending a specially-crafted H.323 traffic, a remote attacker could exploit this vulnerability to cause the device to either reboot normally or reboot into maintenance mode

CVE-2022-20795 CVSS:5.8

Cisco Adaptive Security Appliance and Firepower Threat Defense Software are vulnerable to a denial of service, caused by the suboptimal processing when establishing a DTLS tunnel as part of an AnyConnect SSL VPN connection. By sending a specially-crafted DTLS traffic, a remote attacker could exploit this vulnerability to exhaust resources on the affected VPN headend device and cause DTLS tunnels to stop passing traffic and prevent new DTLS tunnels from establishing.

Impact

- Denial of Service

- Cross-Site Scripting
- Privilege Escalation
- Data Manipulation

Indicators Of Compromise

CVE

- CVE-2022-20786
- CVE-2022-20787
- CVE-2022-20778
- CVE-2022-20788
- CVE-2022-20732
- CVE-2022-20783
- CVE-2022-20795

Affected Vendors

Cisco

Affected Products

- Cisco Unified Communications Manager IM & Presence Service 11.5(1)
- Cisco Unified Communications Manager IM & Presence Service (IM&P) 12.5(1)
- Cisco Unified Communications Manager IM and Presence Service 14
- Cisco Unified Communications Manager 5.1(2b)
- Cisco Unified Communications Manager 6.0(1a)
- Cisco Unified Communications Manager 5.0
- Cisco Unified Communications Manager
- Cisco Webex Meetings
- Cisco Unified Communications Manager Session Management Edition (SME) 11.5
- Cisco Unified Communications Manager 12.5(1)
- Cisco Unity Connection 12.5(1)
- Cisco Unified Communications Manager Session Management Edition (SME) 12.5(1)
- Cisco Virtualized Infrastructure Manager (VIM)
- Cisco RoomOS Software
- Cisco TelePresence Collaboration Endpoint Software
- Cisco Adaptive Security Appliance (ASA) Software 9.16.3
- Cisco Adaptive Security Appliance (ASA) Software 9.17.1.9
- Cisco Firepower Threat Defense (FTD) Software 7.0.1
- Cisco Firepower Threat Defense (FTD) Software 7.1.0.1
-

Remediation

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

CVE-2022-20786 CVE-2022-20787 CVE-2022-20778 CVE-2022-20788 CVE-2022-20732 CVE-2022-20783 CVE-2022-20795