Severity

Medium

Analysis Summary

CVE-2022-20805 CVSS:4.1

Cisco Umbrella Secure Web Gateway could allow a remote authenticated attacker to bypass security restrictions, caused by a flaw in the automatic decryption process. By sending a specially-crafted request, an attacker could exploit this vulnerability to bypass the decryption process.

CVE-2022-20790 CVSS:6.5

Cisco Unified Communications products could allow a remote authenticated attacker to obtain sensitive information, caused by improper input validation in the web-based management interface. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain sensitive information.

CVE-2022-20789 CVSS:4.9

Cisco Unified Communications products could allow a remote authenticated attacker to bypass security restrictions, caused by improper restrictions applied to a system script. By using crafted variables during the execution of a system upgrade, an attacker could exploit this vulnerability to overwrite or append arbitrary data to system files using root-level privileges.

CVE-2022-20804 CVSS:4.3

Cisco Unified Communications products are vulnerable to a denial of service, caused by incorrect processing of certain Cisco Discovery Protocol packets. By sending specially-crafted request, a remote attacker could exploit this vulnerability to cause a kernel panic.

Impact

- Security Bypass
- Information Disclosure
- Denial of Service

Indicators Of Compromise

CVE

- CVE-2022-20805
- CVE-2022-20790
- CVE-2022-20789
- CVE-2022-20804

Affected Vendors

Cisco

Affected Products

- Cisco Umbrella Secure Web Gateway
- Cisco Unified Communications Manager (Unified CM)
- Cisco Unified Communications Manager Session Management Edition (Unified CM SME)
- Cisco Unified Communications Manager Session Management Edition (SME)

Remediation

Refer to Cisco Security Advisory for patch, upgrade or suggested workaround information. CVE-2022-20805 CVE-2022-20790 CVE-2022-20789 CVE-2022-20804