Severity

Medium

Analysis Summary

CVE-2022-20821

Cisco IOS XR could allow a remote attacker to bypass security restrictions, caused by an issue the health check RPM opening TCP port 6379 by default upon activation. By connecting to the Redis instance on the open port, an attacker could exploit this vulnerability to write to the Redis in-memory database, write arbitrary files to the container filesystem, and retrieve information about the Redis database.

Impact

- Security Bypass

Indicators Of Compromise

CVE

- CVE-2022-20821

Affected Vendors

- Cisco

Affected Products

- Cisco IOS XR 7.3.3

Remediation

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

Cisco Security Advisory