

Severity

Medium

Analysis Summary

CVE-2022-20765

Cisco UCS Director is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote authenticated 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.

Impact

- Cross-Site Scripting

Indicators Of Compromise

CVE

- CVE-2022-20765

Affected Vendors

- Cisco

Affected Products

- Cisco UCS Director

Remediation

Refer to Cisco Security Advisory for patch, upgrade or suggested workaround information. [Cisco Security Advisory](#)