UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 0313

## CISCO DISCLOSES ZERO-DAY VULNERABILITY

**DATE ISSUED:** 1st May 2023

| | | | |
|---|---|---|---|
| IMPACT | LOW | MEDIUM | HIGH |
| EASE OF EXPLOIT | HARD | MEDIUM | EASY |

## OVERVIEW

Cisco has disclosed a zero-day vulnerability in its Prime Collaboration Deployment (PCD) software that can be exploited for cross-site scripting (XSS) attacks. Successful exploitation could allow an unauthenticated attacker to launch cross-site scripting attacks remotely, but it would require user interaction.

## BREAKDOWN

A security researcher from NATO Cyber Security Centre (NCSC) discovered a bug in the web-based management interface of Cisco Prime Collaboration Deployment (PCD) version 14 and earlier. This zero-day flaw is tracked as CVE-2023-20060, which originated due to improper validation of user-supplied input in the web-based management interface of PCD. This server management utility enables admins to perform migration or upgrade tasks on servers in their organisation's inventory. An exploit could allow an unauthenticated attacker to execute arbitrary script code allowing access to sensitive information stored in the browser extension.

## REMEDIATION STEPS

- Keep software up to date: Keep operating systems, software applications, and plug-ins updated with the latest security patches
- Monitor network traffic: Use network traffic monitoring tools to identify unusual traffic and behaviour patterns that may indicate malware activity.
- Adopt a 'defence-in-depth' approach that provides layers of defence with several mitigations at each layer.
- Install and regularly update your Next Generation Anti-Virus (NGAV) and anti-malware software that scans computer files to identify and remove malware.

## REFERENCES & RESOURCES

Bleeping Computer https://www.bleepingcomputer.com/news/security/cisco-discloses-xss-zero-day-flaw-in-server-management-tool/