Advisory Alert

Alert Number: AAA20230428 **Date:** April 28, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Medium**	Stack Overflow Vulnerability

Description

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Stack Overflow Vulnerability (CVE-2022-20968)
Description	Cisco has released a security update addressing Stack Overflow Vulnerability in IP Phone models. This vulnerability is due to insufficient input validation of received Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol traffic to an affected device. A successful exploit could allow the attacker to cause a stack overflow, resulting in possible remote code execution or a denial of service (DoS) condition on an affected device Cisco recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	IP Phone 7800 Series IP Phone 8800 Series (except Cisco Wireless IP Phone 8821)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipp-oobwrite-8cMF5r7U

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.