Advisory Alert

Alert Number: AAA20230420 **Date:** April 20, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20154, CVE-2023-20036, CVE-2023-20039)
Description	Cisco has released security updates addressing multiple critical vulnerabilities that exist in their products. **CVE-2023-20154 -** This is a vulnerability that exists due to improper handling of certain messages that are returned by the associated external authentication server. An attacker could exploit this vulnerability by logging in to the web interface of an affected server. Under certain conditions, the authentication mechanism would be bypassed and the attacker would be logged in as an administrator. a successful exploit could allow the attacker to obtain administrative privileges on the web interface of an affected server, including the ability to access and modify every simulation and all user-created data **CVE-2023-20036** - This vulnerability exists due to improper input validation when uploading a Device Pack. An attacker could exploit this vulnerability by altering the request that is sent when uploading a Device Pack. A successful exploit could allow the attacker to execute arbitrary commands as NT AUTHORITY\SYSTEM on the underlying operating system of an affected device. **CVE-2023-20039** - This vulnerability exists due to insufficient default file permissions that are applied to the application data directory. An attacker could exploit this vulnerability by accessing files in the application data directory. A successful exploit could allow the attacker to view sensitive information. Cisco highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cisco Modeling Labs Release versions 2.3, 2.4, 2.5 Cisco IND Release versions prior to 1.11.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cml-auth-bypass-4fUCCeG5 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ind-CAeLFk6V

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20125, CVE-2023-20046, CVE-2023-20004, CVE-2023-20090, CVE-2023-20091, CVE-2023-20092, CVE-2023-20093, CVE-2023-20094, CVE-2023-20098)
Description	Cisco has released a security update addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could cause denial of service, privilege escalation, arbitrary file write, and arbitrary file deletion. Cisco recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cisco BroadWorks Network Server 22.0, 23,0 and Release Independent (RI) ASR 5000 Series Routers, Virtualized Packet Core - Distributed Instance (VPC-DI), Virtualized Packet Core - Single Instance (VPC-SI) that running on Cisco StarOS Software Release 21.22, 21.22.n, 21.23, 21.23.n, 21.25, 21.26, 21.27, 21.27.m, 21.28, or 21.28.m Cisco TelePresence CE and RoomOS Release version 9, 10 and 11 Cisco SD-WAN vManage Software Release versions 20.9, 20.10, 20.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-tcp-dos-KEdJCxLs https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-staros-ssh-privesc-BmWeJC3h https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-file-write-rHKwegKf https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vmanage-wfnqmYhN

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.