Multiple Vulnerabilities in Cisco Catalyst SD-WAN Manager

Severity Level: High

Components Affected

- Cisco Catalyst SD-WAN Manager

Overview

Multiple Vulnerabilities have been reported in Cisco Catalyst SD-WAN Manager which could allow an attacker to access an affected instance or cause a denial of service (DoS) condition on an affected system.

Description

Cisco Catalyst SD-WAN Manager has several vulnerabilities which are described by their CVE number below:

- CVE-2023-20252: Allows an unauthenticated remote attacker to gain unauthorized access to the application using (Security Assertion Markup Language) SAML APIs.

- CVE-2023-20253: Lets an authenticated local attacker with read-only privileges bypass authorization and roll back controller configurations, which could be deployed to downstream routers.

- CVE-2023-20034: Allows an unauthenticated remote attacker to access the Elasticsearch database with Elasticsearch user privileges due to an access control issue in Cisco Catalyst SD-WAN Manager's Elasticsearch implementation.

- CVE-2023-20254: Permits an authenticated remote attacker to access another tenant managed by the same Cisco Catalyst SD-WAN Manager instance through the session management system of the multi-tenant feature.

- CVE-2023-20262: Vulnerability in the SSH service enables an unauthenticated remote attacker to crash a process, causing a denial of service (DoS) condition for SSH access.

Impact

- Denial of Service
- Remote Code Execution
- Information Disclosure
- Elevation of Privilege
- Security Restriction Bypass

Solution/ Workarounds

Apply fixes issued by the vendor;

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vman-sc-LRLfu2z

Reference

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vman-sc-LRLfu2z
- https://www.cert-in.org.in/

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.