### Security Advisory 2023-071

# Cisco Catalyst SD-WAN Manager Vulnerabilities

***September 29, 2023 — v1.0***

**TLP:CLEAR**

*History:*

- *29/09/2023 — v1.0 – Initial publication*

## Summary

On September 27, Cisco issued a Security Advisory for five new vulnerabilities in their `Catalyst SD-WAN Manager` products, with the most critical flaw allowing unauthenticated remote access to the server. `Cisco Catalyst SD-WAN Manager` for WAN is network management software allowing admins to visualise, deploy, and manage devices on wide area networks (WAN) [1].

## Technical Details

The critical vulnerability, labelled `CVE-2023-20252`, with a CVSS score 9.8, permits unauthorised access due to issues with the Security Assertion Markup Language (SAML) APIs. *"A vulnerability in the Security Assertion Markup Language (SAML) APIs of Cisco Catalyst SD-WAN Manager could allow an unauthenticated, remote attacker to gain unauthorised access to the application as an arbitrary user,"* warns Cisco [2].

Attackers can exploit this by sending crafted requests to the SAML APIs, generating arbitrary authorisation tokens for unconditional access. This flaw poses risks such as user impersonation, unauthorised data access, modification, deletion and service disruption.

The other four vulnerabilities are less severe:

- `CVE-2023-20253` (CVSS 8.4): Unauthorised configuration rollback due to CLI vulnerabilities.
- `CVE-2023-20034` (CVSS 7.5): Information disclosure vulnerability in ElasticSearch access control.
- `CVE-2023-20254` (CVSS 7.2): Authorisation bypass in the session management system. (requires multi-tenant feature enabled).
- `CVE-2023-20262` (CVSS 5.3): DoS vulnerability in the SSH service. (affects SSH access only).

Notably, `CVE-2023-20034` is remotely exploitable without authentication, but access is limited to the `Elasticsearch` database with the privileges of the `Elasticsearch` user.

## Affected Products

| Release | CVE-2023-20252 Critical SIR | CVE-2023-20253 High SIR | CVE-2023-20034 High SIR | CVE-2023-20254 High SIR | CVE-2023-20262 Medium SIR |
|---|---|---|---|---|---|
| Earlier than 20.3 | Not affected. | Migrate to a fixed release. | Migrate to a fixed release. | Migrate to a fixed release. | Migrate to a fixed release. |
| 20.3 | Not affected. | Migrate to a fixed release. | 20.3.4 | Migrate to a fixed release. | 20.3.7 |
| 20.4 | Not affected. | Migrate to a fixed release. | Migrate to a fixed release. | Migrate to a fixed release. | Migrate to a fixed release. |
| 20.5 | Not affected. | Migrate to a fixed release. | Migrate to a fixed release. | Migrate to a fixed release. | Migrate to a fixed release. |
| 20.6 | Not affected. | 20.6.2 | 20.6.1 | 20.6.3.4 | Migrate to a fixed release. |
| 20.7 | Not affected. | 20.7.1 | 20.7.1 | Migrate to a fixed release. | Migrate to a fixed release. |
| 20.8 | Not affected. | 20.8.1 | Not affected. | Migrate to a fixed release. | Migrate to a fixed release. |
| 20.9 | 20.9.3.4[1] | 20.9.1 | Not affected. | 20.9.3.2 | 20.9.3 |
| 20.10 | Not affected. | 20.10.1 | Not affected. | 20.10.1.2 | Migrate to a fixed release. |
| 20.11 | Migrate to a fixed release. | 20.11.1 | Not affected. | 20.11.1.2 | 20.11.1 |
| 20.12 | Not affected. | Not affected. | Not affected. | Not affected. | 20.12.1 |

IOS XE Software, SD-WAN cEdge Routers, and SD-WAN vEdge Routers are not vulnerable.

Catalyst SD-WAN Manager version 20.12, tha latest release, is safe except for the medium severity flaw fixed in version 20.12.1.

## Recommendations

No workarounds available, the only recommended action is upgrading to a patched release.

## References

[1] https://www.bleepingcomputer.com/news/security/cisco-catalyst-sd-wan-manager-flaw-allows-remote-server-access/

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

[1] For `CVE-2023-20252`, only releases 20.9.3.2 and 20.11.1.2 are affected. Previous releases in the 20.9 and 20.11 trains are not affected.