

Alert Bulletin

Bulletin N.:

Publication Date: 02/03/2026

Subject: Alert 2026-20 Critical vulnerability in Cisco SD-WAN

Traffic Light Protocol (TLP): Amber

Affected product(s):

The vulnerability affects the following components of Cisco Catalyst SD-WAN:

- **SD-WAN Controller (vSmart)**

Affected versions: 20.3.1 – 20.14.3, 20.15.1

- **SD-WAN Manager (vManage)**

Affected versions: 20.3.1 – 20.14.3, 20.15.1

Applies to on-premises and cloud deployments, including standard, managed, and FedRAMP environments.

Description

A critical vulnerability known as **CVE-2026-20127** (CVSS 10.0) has been reported, which is being actively exploited since 2023. The flaw originates in an error in the peering authentication mechanism of the SD-WAN system.

The vulnerability allows a remote attacker, without the need for credentials or user interaction, to send manipulated requests to bypass authentication. As a result, the attacker can gain access with high privileges and modify the complete SD-WAN network configuration, including:

- Alter network routes
- Add malicious devices or peers
- Manipulate critical configurations

Solution:

Update immediately to the fixed versions:

- **SD-WAN Controller (vSmart)**

Fixed versions: 20.14.4, 20.15.2

- **SD-WAN Manager (vManage)**

Fixed versions: 20.14.4, 20.15.2

Cisco Catalyst SD-WAN Release First fixed version

Before 20.9 ¹	Migrate to a fixed release.
20.9	20.9.8.2
20.11 ¹	20.12.6.1
20.12	20.12.5.3 20.12.6.1
20.13 ¹	20.15.4.2
20.14 ¹	20.15.4.2
20.15	20.15.4.2
20.16 ¹	20.18.2.1
20.18	20.18.2.1

For more information on how to update the SD-WAN, you can follow the following link:

<https://www.cisco.com/c/dam/en/us/td/docs/Website/enterprise/catalyst-sdwan-upgrade-matrix/index.html>

Additional information:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk>
- [Blog elhacker.NET: Critical zero-day vulnerability in Cisco SD-WAN exploited since 2023 to gain root access](#)
- <https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2026-019/>
-