

2026 年 10 月 1 日

内閣官房 国家サイバー統括室
対処調整・官民連携等ユニット**Cisco 製品の深刻な脆弱性 (CVE-2026-76504) について (注意喚起)****1. 対象ソフトウェア**

Cisco Catalyst SD-WAN Manager の以下のバージョンが本脆弱性の影響を受けます。

- ・ 20.9 系: 20.9.10.1 未満
- ・ 20.12 系: 20.12.8.2 未満
- ・ 20.15 系: 20.15.6.1 未満
- ・ 20.18 系: 20.18.4.1 未満
- ・ 26.1 系: 26.1.2.1 未満
- ・ 26.2 系: 26.2.1 未満

2. 脆弱性悪用による影響等

対象製品には、API セッションベースの認証管理に関する脆弱性があり、認証されていないリモートの攻撃者が細工した HTTP リクエストを送信することで認証を回避し、管理者権限で API にアクセスできる可能性があります。

3. 悪用状況

CVE-2026-76504 は、CISA が提供する KEV カタログに追加されており、実際に悪用されていることが確認されています（参考 URL①）。

4. 対応

開発元が提供する情報に基づき、脆弱性が修正されたバージョンにアップデートするとともに、侵害の有無を確認することを強く推奨します（参考 URL②）。

参考 URL

- ① CISA Adds One Known Exploited Vulnerability to Catalog (2026/9/30)
<https://www.cisa.gov/news-events/alerts/2026/09/30/cisa-adds-one-known-exploited-vulnerability-catalog>
- ② Cisco Catalyst SD-WAN Manager API Authentication Bypass Vulnerability
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-sdwan-webauth-xr8beuuU>