TLP:CLEAR【全分野】

別添

2026 年 5 月 15 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 Catalyst SD-WAN 製品の深刻な脆弱性(CVE-2026-20182)について（注意喚起）

1. 対象ソフトウェア

Cisco Catalyst SD-WAN Controller および Cisco Catalyst SD-WAN Manager において、メーカーがサポート（および拡張サポートリリース：ESR）している最新バージョン未満のものが該当します。最新バージョンは以下の通りです。なお、詳細については、参考 URL①をご参照ください。

- 20.9 系(ESR)：20.9.9.1
- 20.12 系(ESR)： 20.12.7.1 / 20.12.6.2 / 20.12.5.4
- 20.15 系(ESR)： 20.15.5.2 / 20.15.4.4
- 20.18 系(ESR)： 20.18.2.2
- 26.1 系： 26.1.1.1

2. 脆弱性悪用による影響等

本脆弱性を悪用することで、認証されていないリモート攻撃者が認証を回避し、該当システムにおける管理者権限を取得する可能性があります。これにより、システムの不正操作や機密情報の漏えいなどの被害が発生するおそれがあります。

3. 悪用状況

CVE-2026-20182 は、CISA が提供する KEV カタログに追加されており、開発元において、脅威アクターによる脆弱性を悪用した攻撃が確認されています（参考 URL②③）。

4. 対応

本脆弱性に対する修正バージョンがリリースされているため、対象ソフトウェアをアップデートし、必要に応じメーカーの手順に従い、侵害の有無を確認することを推奨します（参考 URL①）。また、サポートが終了している製品が残存している場合、最新版への移行や機器の廃止及び後続製品/代替製品への更新を検討することを推奨します。

参考 URL

① Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability (Cisco Systems 社)
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW

② CISA Adds One Known Exploited Vulnerability to Catalog (2026/5/14)
https://www.cisa.gov/news-events/alerts/2026/05/14/cisa-adds-one-known-exploited-vulnerability-catalog

③ Ongoing exploitation of Cisco Catalyst SD-WAN vulnerabilities (2026/5/14)
https://blog.talosintelligence.com/sd-wan-ongoing-exploitation/