TLP:CLEAR【全分野】

別紙

2026 年 7 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

SonicWall 製品の深刻な脆弱性(CVE-2026-15409)について(注意喚起)

1. 対象ソフトウェア

SonicWall 製品の SMA1000 Models - 6210, 7210, 8200v のうち以下のバージョンに該当するもの。

・12.4 系：12.4.3-03245 / 12.4.3-03387 / 12.4.3-03434 (platform-hotfix)
・12.5 系：12.5.0-02283 / 12.5.0-02624 / 12.5.0-02800 (platform-hotfix)

2. 脆弱性悪用による影響等

対象ソフトウェアには、「Work Place」インターフェースにサーバーサイド・リクエスト・フォージェリ（SSRF）の脆弱性があり、認証されていないリモートの攻撃者によって、アプライアンスに意図しない外部または内部の宛先へリクエストを送信させられる可能性があります。

3. 悪用状況

CVE-2026-15409 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）。

5. その他

CVE-2026-15409 に加え、CVE-2026-15410 についても CISA が提供する KEV カタログに追加されています。CVE-2026-15410 は、SMA1000 の管理コンソールに存在する脆弱性であり、管理者権限を有するリモートの攻撃者によって任意の OS コマンドが実行される可能性があります。本脆弱性についても「4. 対応」に記載のアップデートを適用することで解消されます。

参考 URL
① CISA Adds One Known Exploited Vulnerability to Catalog (2026/7/14)
https://www.cisa.gov/news-events/alerts/2026/07/14/cisa-adds-four-known-exploited-vulnerabilities-catalog
② SonicWall Security Advisory: SonicWall SMA1000 Series Appliances Affected By Multiple Vulnerabilities
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008