TLP:CLEAR【全分野】

別紙

2026 年 9 月 3 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-2026-83548 および CVE-2026-83549)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 のうち次のバージョンに該当するもの。

・12.4 系：12.4.3-03453 (platform-hotfix)およびそれ以前のバージョン
・12.5 系：12.5.0-02835 (platform-hotfix)およびそれ以前のバージョン

2. 脆弱性悪用による影響等

CVE-2026-83548 は、Work Place インターフェースにおけるサーバーサイド・リクエスト・フォージェリ（SSRF）の脆弱性であり、認証されていないリモートの攻撃者によって、当該機器から意図しない宛先へリクエストを送信される可能性があります。また、CVE-2026-83549 は、OS コマンドインジェクションの脆弱性であり、管理者権限で認証された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。

3. 悪用状況

CVE-2026-83548 および CVE-2026-83549 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 (2026/9/2)
https://www.cisa.gov/news-events/alerts/2026/09/02/cisa-adds-seven-known-exploited-vulnerabilities-catalog
② SonicWall Security Advisory: SonicWall SMA1000 Series Appliances Affected By Multiple Vulnerabilities
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016