TLP:CLEAR【全分野】

別紙

2026 年 9 月 24 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

F5 製品の深刻な脆弱性(CVE-2026-94127)について(注意喚起)

1. 対象ソフトウェア

- BIG-IP APM (21.x 系) : 21.1.0
- BIG-IP APM (17.5 系) : 17.5.0 以上 17.5.1 以下
- BIG-IP APM (17.1 系) : 17.1.0 以上 17.1.3 以下

2. 脆弱性悪用による影響等

対象ソフトウェアにおいて、BIG-IP APM のアクセスポリシーおよび OAuth プロファイルが同一の仮想サーバーに設定され、OAuth 認可サーバーとして構成されている場合、認証されていないリモートの攻撃者が、バッファオーバーフローの脆弱性を悪用し、任意のコードを実行する可能性があります。

3. 悪用状況

CVE-2026-94127 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 Hotfix を適用するとともに、必要に応じて開発元の手順に従い、侵害の有無を確認することを推奨します（参考 URL②）。

5. 緩和策

開発元より緩和策が提供されています。Hotfix の適用が直ちに困難な場合は、当該緩和策を実施することで本脆弱性の悪用リスクを軽減できます（参考 URL②）。なお、根本的な対策はアップデートの適用であることから、早期のアップデートを強く推奨します。

参考 URL
① CISA Adds Four Known Exploited Vulnerabilities to Catalog (2026/9/22)
https://www.cisa.gov/news-events/alerts/2026/09/22/cisa-adds-four-known-exploited-vulnerabilities-catalog
② K000162605: BIG-IP APM vulnerability CVE-2026-94127
https://my.f5.com/manage/s/article/K000162605