TLP:CLEAR【全分野】

別紙

2026 年 6 月 19 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

Splunk 製品の深刻な脆弱性(CVE-2026-20253)について(注意喚起)

1. 対象ソフトウェア

Splunk Enterprise：10.2.0 ～ 10.2.3 / 10.0.0 ～ 10.0.6

2. 脆弱性悪用による影響等

対象ソフトウェアには、内部で動作するデータ管理コンポーネントである PostgreSQL サイドカーにおいて認証制御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、任意のファイルを作成または削除する可能性があります。さらに、本脆弱性を悪用することで、任意のコマンド実行を可能にする恐れがあります。

3. 悪用状況

CVE-2026-20253 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グレードすることを強く推奨します（参考 URL②）。

5. 緩和策

開発元より緩和策が提示されており、即時のアップデートが難しい場合には、当該緩和策を実施することで本脆弱性のリスクを軽減できます（参考 URL②）。ただし、ソフトウェアの健全性維持の観点から、早期のアップデートを強く推奨します。

参考 URL

① CISA Adds One Known Exploited Vulnerability to Catalog(2026/6/18)
https://www.cisa.gov/news-events/alerts/2026/06/18/cisa-adds-one-known-exploited-vulnerability-catalog

② Unauthenticated Arbitrary File Creation and Truncation in a PostgreSQL Sidecar Service Endpoint in Splunk Enterprise
https://advisory.splunk.com/advisories/SVD-2026-0603