TLP:CLEAR【全分野】

別紙

2026 年２月 16 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

FileZen の深刻な脆弱性(CVE-2026-25108)について(注意喚起)

1. 対象ソフトウェア

・FileZen
- V4.2.1 から V4.2.8
- V5.0.0 から V5.0.10

※物理版、仮想版ともに影響を受けます。
※FileZen ウイルスチェックオプションが有効になっている、かつ攻撃者が何らかの方法（漏えいしたログオン情報の利用、等）によりユーザーログオンできる状態である場合、本脆弱性の影響を受けます。

2. 脆弱性悪用による影響等

対象ソフトウェアに対して、遠隔の第三者により任意の OS コマンドを実行される恐れがあります。

3. 悪用

開発元において、顧客環境に対する脆弱性を悪用した攻撃が１件以上確認されています（参考 URL①）。

4. 対応

対象ソフトウェアの V5.0.11 以降へのアップデートを強く推奨します。また、FileZen ウイルスチェックオプションを無効にすることやユーザーのログイン ID・パスワードを変更することも強く推奨します。

5. その他

開発元より、対象ソフトウェアのアップデートは 2026 年 3 月末をもって終了する旨の周知がなされていることから、代替製品の検討を早急に実施することを強く推奨します（参考 URL②）。

参考 URL
① 【重要】FileZen ログオン後画面でのコマンドインジェクション脆弱性について
https://www.soliton.co.jp/support/2026/006657.html
② 販売終了製品のサポート情報
https://www.soliton.co.jp/support/support_eos_product.html
③ FileZen における OS コマンドインジェクションの脆弱性（CVE-2026-25108）に関する注意喚起
https://www.jpcert.or.jp/at/2026/at260004.html