サポートからのお知らせ

【重要】FileZen設定内容確認のお願い

2021年03月05日

(2021/03/05更新：脆弱性修正済みアップデートファームウェアのリリースを記載)
FileZenに新たな脆弱性が存在することを確認しました。
FileZenをご利用のお客様は、必ず以下に記す設定をご確認いただき、必要な対策を実施いただきますようお願い申し上げます。

新たに確認した脆弱性は、システム管理者としてログオンしているセッション内に限り発現するものです。しかしながら、V4.2.2までの脆弱性を利用しFileZenに侵入された場合、パスワードを窃取する手法があることも確認しています。
アクセス制御が適切に行われていない場合、窃取されたパスワードと今回発見した脆弱性を利用することで、FileZenへの侵入される恐れがあります。
従いまして、以下に記す対策を実施いただきますよう強くお願い申し上げます。

1．対策方法

・システム管理者アカウントの変更
・アクセス制御の再設定
・本脆弱性が修正されているバージョンにする

2．対象製品とバージョン

・FileZen V3.0.0からV4.2.7までの各バージョン
・FileZen V5.0.0からV5.0.2までの各バージョン

3．確認した脆弱性と影響

（1）確認した脆弱性
OSコマンドインジェクションの脆弱性
なお、今回確認した脆弱性を「情報セキュリティ早期警戒パートナーシップ」に基づく自社製品の脆弱性としてJPCERT/CCを通じて制度に届け出ました。
(CVE-2021-20655)
CVSS v3　CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H　基本値: 9.1
CVSS v2　AV:N/AC:L/Au:S/C:C/I:C/A:C　基本値: 9.0

（2）脆弱性の影響
FileZenのシステム管理者画面にログオンした状態から、FileZenを不正に操作することが可能です。
この脆弱性を利用した攻撃が成立した場合、FileZenにアップロードしたファイルが窃取される、踏み台にされさらなる攻撃に悪用される可能性があります。

（3）(本件に限らない)脆弱性の危険性
FileZenをお使いいただくなかで、
・アクセス制御設定が意図通りに設定されていない
・過去に既知の脆弱性を利用され攻撃被害を受けていたが、そのことに気付かずに認証情報を窃取された
などの可能性があります。
ご利用のFileZenが脆弱な状態である可能性があるため、対策手順に従い確認および再設定を実施してください。

4．本脆弱性修正済みバージョン

2021年3月5日に以下アップデートファームウェアをリリースしました。
ST82用：V5.0.3・V4.2.8
ST81/DX51用：V4.2.8

※ 本脆弱性に対するファームウェアです。前項(3)に記す危険性は修正済みファームウェアでも対応できません。
必ず、修正済みファームウェア適用とは別に速やかに対策手順の対応をお願いいたします。

5．対策手順

対策は、「システム管理者アカウントの認証情報が窃取されているかもしれない」ことを前提に、
・新たなシステム管理者の作成と「admin」無効化 (5-1)
・「admin」以外の既存システム管理者アカウントの降格または削除 (5-2)
を実施してください。
また、外部からシステム管理者によるログインができないよう
・システム管理者のアクセス制御に関する設定 (5-3)
を実施してください。

※ 設定内容確認ならびに対策において、(ファームウェア適用を除き)再起動等は必要なく、システム停止(サービスダウンタイム)は生じません。また、長時間かかるものでもないため全てのお客様にてできるだけ早く実施ください。

5-1 新たなシステム管理者の作成と「admin」無効化

以下の手順で、新たにシステム管理者を作成し、初期管理者アカウント「admin」を無効化してください。

※ 新たに作成したシステム管理者アカウントに対して、「5-3 システム管理者のアクセス制御に関する設定」を忘れずに実施してください。

＜FileZenサービスページ（システム管理者アカウントの作成）＞

（1） [管理者]-[ユーザー管理]-[一覧表示](図1)で、システム管理者権限を設定するユーザーを作成します。

サポート

ダウンロード
FAQ
サービスメニューのご紹介
OS・仮想基盤・ウイルス対策ソフト対応状況
サポート対象バージョン
販売終了製品のサポート
サポートポリシー
クラウドサービスのサポートポリシー
製品の輸出について

お知らせ
サポートからのお知らせ
アップデートのお知らせ

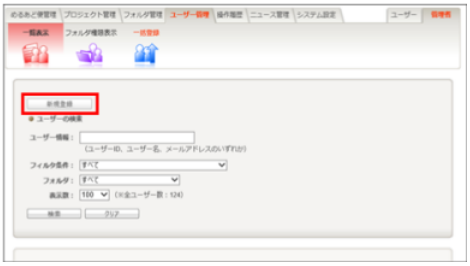

図1　ユーザーの一覧表示

（2）　[管理者]-[システム設定]-[管理者設定]（図2）で、作成したユーザーにシステム管理者の権限を設定します。

図2　管理者追加設定

（3）　[設定したユーザーでFileZenサービスにログオンして、[管理者]タブにアクセスできることを確認します。

＜システム管理ページ（adminの無効化）＞

（4）　[サービス]-[サーバー状態]「サービス操作」（図3）で、「FileZenサービスのシステム管理者(admin)に関する操作」の「無効にする」の<実行>をクリックします。

図3　（システム管理ページ）サービス操作

5-2 「admin」以外の既存システム管理者アカウントの降格または削除

「admin」以外の既存のシステム管理者アカウントが存在する場合、そのアカウントをシステム管理者以外の用途に利用している場合は降格、システム管理者のみの利用であった場合は削除を行います。以下の手順は、5-1で新規作成したシステム管理者アカウントでFileZenサービスページにログオンし直して行います。

＜既存システム管理者アカウントを他の用途でも利用していた場合＞

既存システム管理者アカウントを、一般のめるあど便やプロジェクト利用等で利用していた場合は、削除ではなく降格を行います。[管理者]-[システム設定]-[管理者設定]（図4）で、当該ユーザーを検索し、チェックを外し「次へ」を押下して、次の画面で「変更する」を押下して下さい。このユーザーはシステム管理者ではないアカウントとなります。この後、パスワード変更も必ず実施して下さい。

図4 システム管理者一覧

＜既存システム管理者アカウントを管理者専用で利用していた場合＞

既存システム管理者アカウントを管理者専用で利用していた場合はアカウントの削除を行います。[管理者]-[ユーザー管理]-[一覧表示](図5)で当該ユーザーを検索し、対象のアカウントの[操作]にある[削除]を押下します。

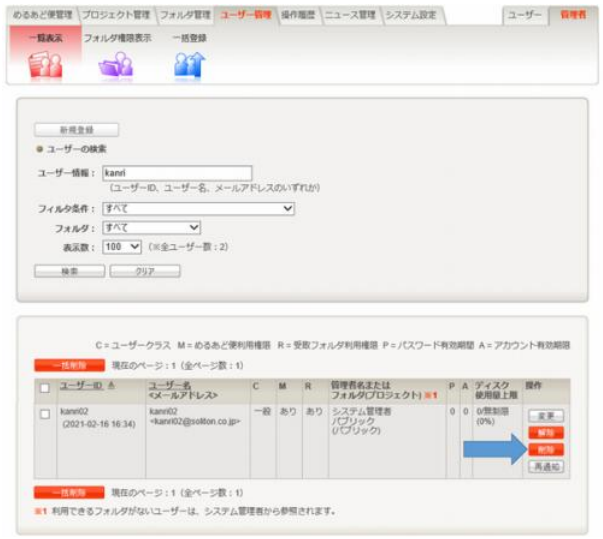

図5 ユーザー一覧

5-3 システム管理者のアクセス制御に関する設定

システム管理者のアクセス制御に関する設定は、
・アカウントに対する設定
・システム設定からの設定
の2カ所にあります。
また、システム設定においては、
・システム管理者
・APIからのアクセス
・FileZen Relay Agent
の3カ所すべてを設定する必要があります。

なお、「アカウントの設定」と「システムの設定」では「アカウントの設定」が優先されますが、設定漏れを考慮し、双方に設定することを推奨します。

＜FileZenサービスページ(システム管理者アカウントに対する設定)＞

(1) 5-2(2)の手順でシステム管理者アカウントを確認します。

(2) [管理者]-[ユーザー管理]-[一覧表示](図5)で5-3(1)の手順でシステム管理者アカウントを確認し[操作]にある[変更]を押下します。

(3) [アクセス元IPアドレスの検証]に組織内ネットワークなどの管理者アクセスに必要なIPアドレス(または範囲)を入力します。(図6)

図6 アカウント設定

（4） [管理者]-[システム設定]-[アクセス制御]（図7）で[編集]から設定を行います。
組織内ネットワークなどのアクセスに必要なIPアドレス(または範囲)を入力します。

図7 アクセス制御設定

・[システム管理者]
″Webブラウザを利用してアクセスするシステム管理者の接続元IPアドレスを設定します。

・[APIからのアクセス]
API(現在非公開)やFileZen Mobile、およびSoliton SecureBrowser / WrappingBoxのFileZen連携を利用してアクセスするシステム管理者を含めた全てのアカウントが対象です。
FileZen Mobileを利用し、インターネットからアクセスする場合は、この設定は空欄にし、必ず5-3（1）から（3）の手順で全てのシステム管理者アカウントに対して適切なIPアドレス制限設定を行って下さい。
Soliton SecureBrowser / WrappingBoxのFileZen連携を利用している場合、Soliton SecureGatewayのIPアドレス（FileZenとの経路上に上位プロキシが存在する場合にはその機器のIPアドレス）を指定してください。
この機能を利用しない場合は、″127.0.0.1″を設定してください。

・[FileZen Relay Agent]
FileZen Client、FileZen RA、FileZen FileConversionを利用してアクセスするシステム管理者を含めた全てのアカウントが対象です。
FileZen Client、FileZen FileConversionを利用する接続元IPアドレスを設定します。
FileZen RAを使用している場合、FileZen RAをインストールしている Windows サーバーの IP アドレスを指定してください。
この機能を利用しない場合は、″127.0.0.1″を設定してください。

5-4 設定に関する注意事項

（1） ユーザーのメールアドレスについて
FileZenのユーザーのメールアドレスは重複ができません。「通知メール設定」で設定した「管理者のメールアドレスの設定」は、adminで設定したメールアドレスに連動しています。そのため、新たに追加する管理者のメールアドレスには違うメールアドレスを設定して下さい。

（2） アクセス元IPアドレスの検証について
機器とFileZenの間にProxyサーバーやNAT装置がある場合、FileZenから見える機器のIPアドレスは実際のものと違っている場合があります。「アクセス元IPアドレスの検証」には、FileZenに届く通信のソースIPアドレスで設定下さい。

6. より安全にお使いいただくために

FileZenを安心して、より安全にお使いいただくために以下もあわせてご検討ください。

6-1 最新のファームウェアを適用する

新しいファームウェアには、機能には影響しない修正も含まれます。これらの修正により未知の脆弱性が結果として修正されることがあります。(CVE-2020-5639はこのケースに該当します) そのため、リリースノートを参照し脆弱性修正がないから適用しない、ではなく常に最新のファームウェアを適用することを推奨します。

6-2 シスログを出力する

FileZen V4.2.2以降のバージョンでは、攻撃行為を検知するために有用なログが出力できます。
攻撃者は攻撃行為を気付かれないように、慎重に長期間侵入することが多くあります。そのため、攻撃発見時には大きな被害を受けていたとならないように、外部サーバーへログを出力することと、ログを監視することを推奨します。
出力するログの詳細に関しては、「FileZen システム管理ページリファレンスマニュアル」の「付録6 ハードウェア情報/監視ログ ログメッセージ一覧」を参照ください。

6-3 電子証明書認証を利用する

FileZenはクライアント電子証明書の検証を行い、認証をより強化することができます。
パスワードはそのシステムから漏洩していなくとも、他のシステムから漏洩することもありますので、電子証明書を利用した認証強化もご検討ください。

6-4 FileZen利用ユーザーのパスワードを変更する

電子証明書認証を利用していない環境では、FileZenだけに関わらず「パスワードは流出するもの」の考えを前提に、利用ユーザーもパスワードを変更することを推奨します。
また、パスワードを変更する際には、「パスワードを流用しない」「前のパスワードから推測されるパスワードを利用しない」などパスワードの運用にはご注意ください。

用語集

FileZen RA
Windowsファイルサーバー経由でFileZenプロジェクトフォルダへファイルのアップロード・ダウンロードを自動で行うためのソフトウェア(有償)。

FileZen Client
WindowsクライアントからFileZenプロジェクトフォルダへファイルをアップロード・ダウンロードを自動で行うためのソフトウェア(有償)。

FileZen FileConversion
FileZenプロジェクトフォルダへファイルをアップロードする際、PDFファイルに変換するソフトウェア(有償)。
通称:FileZen PDFコンバーター

FileZen Mobile
iOS、Android向けのFileZenのクライアントアプリ(無償)。

API
FileZenの持つWeb-API。
以前は案件ベースで一部のお客様に仕様を開示していましたが、FileZen Client等のリリースによりお客様への開示は終了しています。
FileZen Mobile、およびSoliton SecureBrowser/WrappingBoxのFileZen連携もこのWeb APIを使用しています。

以上