【Create!Form】Java証明書の脆弱性に関する対処について

2026年11月9日
インフォテック株式会社

本資料は、Create!Form Magicfolder／Magicfolder Plus／RemoteObjectに同梱されているJavaの証明書に関する脆弱性と、その対処方法をまとめたものです。対象製品と、証明書の削除手順を以下に記載します。

項目	内容
Create!Form製品名	Magicfolder／Magicfolder Plus／RemoteObject
対象バージョン	V12.0／V12.1／V12.2／V12.3
対象OS	Windows／Linux（S2版を含む）

■ 1. 対象の脆弱性

公表日	脆弱性番号	問題と対策の内容
2026年10月21日	**CVE-2026-91403**	侵害されたeMudhraの中間認証局に関連する証明書を、Javaが信用してしまうおそれがある問題です。相手になりすました偽の証明書を受け入れると、通信内容の盗み見・改ざんにつながるおそれがあります。公式告知
2026年10月24日	**CVE-2026-114820**（JDK-8395690）	同じ証明書事故に関連し、信頼ストアから対象4ルートを削除する追加対策です。公式告知

■ 2. 作業前の確認

作業には、対象ファイルを更新できる管理者権限が必要です。

対応が必要なファイルは、製品に同梱されている`vender`フォルダー内の以下のファイルです。 対処には、`cacerts`ファイル内の対象証明書を削除します。**`cacerts`ファイル自体は削除しないでください。**

OS	Javaの配置	証明書ストア
Windows	`vender\Jre`	`vender\Jre\lib\security\cacerts`
Linux	`vender/jre`	`vender/jre/lib/security/cacerts`

対象ルートで発行された正当な証明書も、信用されなくなる場合があります。作業後は、実際に使用しているHTTPS連携やメール送信などを確認してください。

■ 3. 削除対象の証明書

削除対象は次の4種類です。同梱Javaによって登録されている証明書の種類や登録名が異なり、バージョンによっては一部が元から登録されていません。

ルート証明書の名前
emSign Root CA - G1
emSign Root CA - G2
emSign ECC Root CA - G3
AAA Certificate Services

コマンドは証明書の指紋（SHA-256）または証明書名で対象を判定して削除し、削除後に対象の証明書が残っていないことを確認します。元から登録されていない証明書は削除せず、処理を続けます。

■ 4. 対処方法（Windows）

配布ファイル`CreateFormCertWorkaround.zip`を保存し、次の準備をしてください。

1. ZIPファイルを右クリックして「プロパティ」を開きます。「許可する」が表示されている場合はチェックを入れ、「適用」をクリックしてください。
2. ZIPファイルを右クリックして「すべて展開」を選び、展開先に`C:\CreateFormCertWorkaround`を指定してください。
3. スタートメニューで「Windows PowerShell」を検索し、右クリックして「管理者として実行」を選んでください。 ※ PowerShellが使える環境で実行してください

スクリプトファイルは編集せず、そのまま使用してください。

4.1 サービスを停止する

1. ジョブの新規受付を止め、処理中のジョブが完了するまで待ってください。
2. Windowsのサービス管理画面で管理画面サービス（サービス名：`cfccd12`）を停止してください。

4.2 バックアップ・証明書の削除・確認を実行する

`mfro-remove-certificates.ps1`を使用します。管理者PowerShellで、次の1行を実行してください。

```
powershell.exe -NoProfile -ExecutionPolicy RemoteSigned -File "C:\CreateFormCertWorkaround\scripts\windows\mfro-remove-certificates.ps1"
```

導入先は環境変数から自動で取得し、`INFO: 導入先：`に表示します。表示された導入先が作業対象であることを確認し、`Y`を入力してEnterキーを押してください。`Y`以外を入力すると、ファイルを変更せず

に中止します。続いて、バックアップの作成、対象証明書の削除、削除後の確認まで実行します。

`Certificate removal and verification completed.` と表示されたら、表示されたバックアップと証明書一覧のフルパスを控え、4.3へ進んでください。エラーで停止した場合は、サービスを停止したまま、表示内容を確認してください。

4.3 サービスを再開する

サービスを再開し、正しく動作することを確認してください。

■ 5. 対処方法（Linux）

配布ファイル `CreateFormCertWorkaround.zip` をLinuxサーバーへ転送し、任意のフォルダーへ展開してください。展開したフォルダーでBashを開き、rootまたは対象ファイルを更新できる管理者として作業します。S2版も同じファイルを使用します。

5.1 サービスを停止する

1. ジョブの新規受付を止め、処理中のジョブが完了するまで待ってください。
2. 通常の運用手順に従って管理画面サービスを停止してください。

5.2 バックアップ・証明書の削除・確認を実行する

`mfro-remove-certificates.sh` を使用します。ZIPを展開したフォルダーで、次の1行を実行してください。

```
bash scripts/linux/mfro-remove-certificates.sh
```

`Create!Form installation directory` で始まる入力案内が表示されます。導入ディレクトリーのフルパス（入力例：`/opt/createv12`）を入力し、Enterキーを押してください。

`Certificate removal and verification completed.` と表示されたら、バックアップと証明書一覧のフルパスを控え、5.3へ進んでください。`ERROR:` で停止した場合は、サービスを停止したまま、表示内容を確認してください。

5.3 サービスを再開する

サービスを再開し、正しく動作することを確認してください。

■ 6. エラーが出た場合・元に戻す場合

表示・状況	対応
アクセス拒否／Permission denied	実行権限・対象ファイルの書き込み権限を確認してください。
「デジタル署名されていません」「スクリプトの実行が無効」（Windows）	ZIPファイルの展開時に、4の準備の手順1（ZIPファイルのプロパティで「許可する」にチェック）を実行していない可能性があります。展開済みのフォルダー（`C:\CreateFormCertWorkaround`）を削除し、手順1を実行してから、もう一度展開してください。
対処後にHTTPSやメール接続が失敗する	対象ルートに依存していた可能性があります。
バックアップファイルが複数できている	スクリプトを実行するたびに、バックアップが作成されます。一番古いファイル（ファイル名の日時が最も古いもの）に戻すことで、今回の対処前の状態に戻せます。

誤操作などで元に戻す必要がある場合は、業務受付を止め、4.1または5.1に従ってサービスを停止してから、バックアップファイルを元の証明書ストアへコピーしてください。

バックアップを復元すると、削除した証明書への信頼も戻り、今回の対処前の状態になります。

バックアップは証明書ストアと同じフォルダーに、`cacerts.before-emudhra-`で始まる名前で保存されます。ファイル名を確認し、削除前に作成したバックアップのフルパスを指定してください。作業を再実行した際のバックアップは、初回の削除前の状態とは限りません。

6.1 Windowsでバックアップを復元する

4.1に従ってサービスを停止してから、`mfro-restore-certificates.ps1`を実行します。管理者PowerShellで、次の1行を実行してください。

```
powershell.exe -NoProfile -ExecutionPolicy RemoteSigned -File "C:\CreateFormCertWorkaround\scripts\windows\mfro-restore-certificates.ps1"
```

導入先は環境変数から自動で取得し、`INFO: 導入先：`に表示します。表示された導入先が作業対象であることを確認し、`Y`を入力してEnterキーを押してください。続いてバックアップのフルパスを聞かれたら、表示された入力例を参考に、削除前に作成したバックアップファイルのフルパスを入力してEnterキーを押してください。

6.2 Linuxでバックアップを復元する

5.1に従ってサービスを停止してから、`mfro-restore-certificates.sh`を実行します。ZIPを展開したフォルダーで、次の1行を実行してください。

```
bash scripts/linux/mfro-restore-certificates.sh
```

最初に、導入ディレクトリーのフルパス（入力例：`/opt/createv12`）を入力してEnterキーを押してください。続いて`Backup file`で始まる入力案内が表示されたら、表示された入力例を参考に、削除前に作成したバックアップファイルのフルパスを入力してEnterキーを押してください。

`Restore completed.`と表示されたら、4.3または5.3に従ってサービスを再開し、正しく動作することを確認してください。エラーで停止した場合は、サービスを停止したまま、表示内容を確認してください。

■ お問い合わせ

本件に関するお問い合わせは、Create!Formユーザーサポートサイトよりお問い合わせください。