

お知らせ



ホーム > サポート > お知らせ > [至急]Proselfのゼロデイ脆弱性による攻撃発生について

[至急]Proselfのゼロデイ脆弱性による攻撃発生について

お知らせカテゴリー

- > 全て
- > 重要
- > 障害情報
- > お知らせ
- > リリース情報
- > マニュアル
- > ブラウザ別サポート情報

2023/10/10

平素はProselfをご利用いただき、誠にありがとうございます。

弊社製品であるProselfにおきまして新たなゼロデイ脆弱性が発見されました(2023/10/04付)。脆弱性の内容としてはXXE(XML External Entity)となります。攻撃者はXXEを悪用してProselfのアカウント情報を外部に送信し、その情報を元にProselfへの不正ログインを試みている可能性がございます。

本脆弱性は以下のバージョンに含まれます。

- Proself Ver5.62以下
- Proself Gateway Edition Ver1.65以下
- Proself Mail Sanitize Edition Ver1.08以下

既に本脆弱性が悪用されていることを確認しておりますため、Proselfをご利用中のお客様におかれましてはお手数をおかけし誠に申し訳ございませんが、以下について急ぎご確認をお願い申し上げます。

【目次】

- 攻撃を受けたかどうかの確認
- 暫定対応について
- 恒久策について
- Proselfのゼロデイ脆弱性への対応バージョンに関する補足

攻撃を受けたかどうかの確認

以下の手順にてご確認ください。

◆Linux OSの場合

1. コンソールを起動後、Proselfインストールフォルダ/logs に移動します。(赤文字部分)
以下はProselfインストールフォルダが「/usr/local/Proself5」である場合の例となります。

```
# cd /usr/local/Proself5/logs
```

※Proselfインストールフォルダについては以下FAQに記載している手順で確認できます。
<https://www.proself.jp/support/faq433/>

2. 以下コマンドを実行します。(赤文字部分)

```
# grep "jp.co.northgrid.proself.updater.afterreboot.logic.AfterRebootCheckLogic - .*Proself Ver" proself_updater.log*
```

※改行を含めず必ず1行にして実行ください。
また、ダブルクォーテーション内の半角スペースが以下のようにになっているかどうかを必ずご確認ください。
(略)AfterRebootCheckLogic(半角スペース)(半角スペース)-(半角スペース).*Proself(略)

◆Windows OSの場合

1. コマンドプロンプトを起動後、Proselfインストールフォルダ/logs に移動します。(赤文字部分)
以下はProselfインストールフォルダが「C:\Program Files\Proself5」である場合の例となります。

```
C:>cd "C:\Program Files\Proself5\logs"
```

※Proselfインストールフォルダについては以下FAQに記載している手順で確認できます。
<https://www.proself.jp/support/faq433/>

2. 以下コマンドを実行します。(赤文字部分)

```
C:\Program Files\Proself5\logs>findstr /R  
/C:"jp.co.northgrid.proself.updater.afterreboot.logic.AfterRebootCheckLogic - .*Proself Ver" proself_updater.log*
```

※改行を含めず必ず1行にして実行ください。
また、ダブルクォーテーション内の半角スペースが以下のようにになっているかどうかを必ずご確認ください。

ください。

(略)AfterRebootCheckLogic(半角スペース)(半角スペース)-(半角スペース).*Proself(略)

上記コマンド実行結果の見方は以下の通りとなります。

- **コマンド実行時に出力がある場合**

以下のような出力がある場合は攻撃が行われた可能性がございます。

```
proself_updater.log:ERROR 2023-10-05 00-00-00: 864643784 [https-jsse-nio-443-exec-14] jp.co.northgrid.proself.updater.afterreboot.logic.AfterRebootCheckLogic - 「Proself Ver (何らかの文字列)」
```

出力がある場合は影響有無の確認等を弊社で行いたく存じますので、大変恐れ入りますが「info@proself.jp」までご連絡いただくか、以下弊社お問い合わせフォームよりお問い合わせください。よろしくお願いいたします。

※その他、万が一疑わしいログがあった場合は弊社にご連絡ください。

→[弊社お問い合わせフォーム](#)

- **コマンド実行時に何も出力がない場合**

攻撃は行われておりません。

暫定対応について

以下の手順を実施ください。

- 暫定対応については脆弱性が悪用されたどうかに関わらず**全てのお客様が対象**ですので、必ず実施くださいますようお願い申し上げます。
- Proselfのサービス再起動は不要で即時反映されます。
- 本対応によるProselfのご利用ユーザーに対する影響はございません。

1. 以下のダウンロードURLにアクセスし「updaterafterreboot.xml」をダウンロードします。

◆**ダウンロードURL**

<https://support.proself.jp/public/tAIqAwIAvqA2rIEAT4ffrY7laqegWFKh-foM>

上記アクセス時にメールアドレスを入力し「パスワードを取得」をクリックしますと、パスワードの入力画面に切り替わると共にワンタイムパスワードが記載されたメールが送信されます。画面上のパスワード欄にワンタイムパスワードを入力の上「パスワード送信」をクリックください。

2. ダウンロードした「updaterafterreboot.xml」を「◆ダウンロードしたファイルの上書き先」に記載しているフォルダ内に**上書きコピー**します。

◆**ダウンロードしたファイルの上書き先**

```
Proselfインストールフォルダ/webapps/proself/WEB-INF/xml/process/admin/config/
```

※Proselfインストールフォルダについては以下FAQに記載している手順で確認できます。

<https://www.proself.jp/support/faq433/>

◆**Linux OSの例**

Proselfインストールフォルダが「/usr/local/Proself5」である場合は、「updaterafterreboot.xml」の上書き先は以下のようになります。

```
/usr/local/Proself5/webapps/proself/WEB-INF/xml/process/admin/config/
```

◆**Windows OSの例**

Proselfインストールフォルダが「C:¥Program Files¥Proself5」である場合は、「updaterafterreboot.xml」の上書き先は以下のようになります。

```
C:¥Program Files¥Proself5¥webapps¥proself¥WEB-INF¥xml¥process¥admin¥config¥
```

恒久策について

本脆弱性に対応したアップデート版をリリースいたします。リリースし次第あらためてProselfホームページ上およびメールにてご案内申し上げますので、しばらくお待ちくださいますようお願い申し上げます。

この度はご迷惑をおかけし誠に申し訳ございません。

Proselfのゼロデイ脆弱性への対応バージョンに関する補足

次期バージョンリリースの対象につきましては以下の通りとなりますことを補足申し上げます。

- 以下は現在サポート中のため、脆弱性対応を行ったバージョンをリリースいたします。
 - Proself Enterprise Edition Ver.5
 - Proself Standard Edition Ver.5
 - Proself Gateway Edition Ver.1

- Proself Mail Sanitize Edition Ver.1
- 以下はサポート終了しているため、脆弱性対応を行ったバージョンのリリースは行いません。
 - Proself Enterprise Edition Ver.4以下
 - Proself Standard Edition Ver.4以下

【ご注意】
 Ver.4以下(Enterprise Edition/Standard Edition)をご利用中の場合、Proselfのご利用を停止するかVer.5へのバージョンアップをご検討ください。サポートが終了しているバージョンをそのまま利用し続けた場合、脆弱性を悪用され全てのファイルが流出してしまう危険性がございます。

サポートに関しては「Proself年間保守サービス規約」に基づいております。規約については以下のURLをご参照ください。
<https://www.proself.jp/pdf/proselfsupport.pdf>
 ※規約は保守サービスライセンス証書の裏面に印刷されているものと同様です。

以上

戻る

機能紹介	事例紹介	オプション	価格	サポート	トライアル
<ul style="list-style-type: none"> ▶ ファイル操作 ▶ ファイル受け渡し ▶ グループアクセス ▶ マルチデバイスアクセス ▶ セキュリティ ▶ 管理機能 	<ul style="list-style-type: none"> ▶ 企業 ▶ 大学・教育機関 ▶ 官公庁・独立行政法人 ▶ SIベンダー・販社様へ ▶ ファイル受け渡し ▶ ファイル共有 ▶ リモートアクセス ▶ ネットワーク分離環境 ▶ 企業様 ▶ 大学様 	<ul style="list-style-type: none"> ▶ スマートフォンオプション ▶ Mail Proxy オプション ▶ レポートオプション ▶ 統合認証オプション ▶ 文書内検索オプション ▶ SAML認証オプション ▶ CAS認証オプション ▶ Proself Client ▶ 同期ツール ▶ Proself Client (iOS版) ▶ Proself Client for Android ▶ Proself Disk 	<ul style="list-style-type: none"> ▶ 本体・オプション価格 ▶ サポート価格 ▶ 動作環境 ▶ ブラウザ別サポート情報 ▶ ご購入 	<ul style="list-style-type: none"> ▶ お知らせ ▶ FAQ ▶ お問い合わせ ▶ ダウンロード ▶ マニュアル ▶ ユーザー登録 	<ul style="list-style-type: none"> ▶ インストール版 ▶ オンライン版 ▶ その他 ▶ 会社情報 ▶ 特定商取引法に基づく表記 ▶ 個人情報の取扱いについて

