JVN#86350682 SHIRASAGI におけるオープンリダイレクト脆弱性とクロスサイトスクリプティング脆弱性

JPCERT コーディネーション センターと独立行政法人情報処理推進機構 (IPA)が共同運営するJVNに、SHIRASAGI におけるオープンリダイレクト脆弱性とクロスサイト・スクリプティング脆弱性が公開されました。

https://jvn.jp/jp/JVN86350682/index.html

オープンリダイレクト脆弱性（CVE-2022-43479）

この脆弱性をついた攻撃を成立させるには、下記の条件が必要となります。

シラサギのログイン画面URLにrefパラメータとして任意のサイトのURLをつけたリンクをクリックさせます（以下例）refパラメータで指定したサイトにリダイレクトする（被害者は認証不要）。

https//www.example.jp/.mypage/login?ref=https://xxxx
https//www.example.jp/.mypage/redirect?ref=https://xxxx
https//www.example.jp/.g1/schedule?calendar%5Bpath%5D=https://xxx

この脆弱性を悪用すると、任意のサイトにリダイレクトさせることが可能となるため、フィッシング被害などを被る可能性があります。

クロスサイト・スクリプティング脆弱性（CVE-2022-43499）

この脆弱性をついた攻撃を成立させるには、下記の条件が必要となります。

1. SHIRASAGI にクロスサイト・スクリプティング脆弱性が組み込まれた SVG ファイルをアップロードする。次のような順で SVG ファイルをアップロードすることができる。
   1. 管理画面にログインし、左メニューの「ファイル」から SVG ファイルをアップロードする（https://demo.ss-proj.org/.u/user_files）
   2. CMS のアップロードフォルダーに SVG ファイルをアップロードする（https://demo.ss-proj.org/.s1/uploader153/files/img）
2. アップロードしたファイルの URL を HTML などから取得し、ブラウザで URL を表示する。
3. SVG ファイルに組み込まれたクロスサイト・スクリプティング脆弱性が発生する。

この脆弱性は全てのバージョンのSHIRASAGIに存在します。

修正方法

修正方法は、SHIRASAGI本体の更新に加え nginx 設定（apache httpd をご利用の場合は apache httpd 設定）の変更が必要で、手順は以下の通りとなります。

1. SHIRASAGI 開発マニュアルのSHIRASAGI の更新を参考にSHIRASAGI本体をv1.16.2へバージョンアップする。
2. nginx をご利用の方は、SHIRASAGI 開発マニュアルのNginx のインストールの(2) プロキシーの設定を参考に、SVG ファイルに対して "Content-Disposition: attachment" ヘッダを付与するように修正。
3. apache httpd をご利用の方は、SHIRASAGI 開発マニュアルのApache のインストールの(2) VirtualHost設定を参考に、SVG ファイルに対して "Content-Disposition: attachment" ヘッダを付与するように修正。

新着情報

- LGWAN-ASPのインターネット連携オプションについて
- v1.14.0の留意事項について
- v1.14.1の不具合修正について
- シラサギ v1.13.0 リリース延期のお知らせ
- サーバーメンテナンスのお知らせ
- 操作マニュアルを追加しました。
- JVN#74699196 SHIRASAGI におけるオープンリダイレクトの脆弱性
- シラサギ v1.11.0リリースに伴う操作マニュアルの更新について
- シラサギ v1.11.0 リリース延期のお知らせ
- 操作マニュアルを追加しました。

シラサギ
LGWAN-ASPサービス

シラサギ
クラウドサービス

シラサギ
業務代行サービス

シラサギ
講習会サービス

シラサギ
サポートサービス

カテゴリー | その他

サイトマップ | プライバシーポリシー | お問い合わせ | 協業ベンダーの皆様