UCHIDA

実績に基づくIT資産管理ソフトウェア
ASSETBASE

ASSETBASE システムのクロスサイトスクリプティング脆弱性のご報告と

セキュリティ強化プログラムのリリースについて

公開日　2017 年 4 月 10 日

平素は、IT 資産管理システム ASSETBASE をご利用いただき、誠にありがとうございます。
JPCERT コーディネーションセンターより、ASSETBASE Ver.8.0 およびそれ以前のシステムに存在する、クロスサイトスクリプティングの脆弱性の指摘を受けました。この脆弱性の影響、および対策・回避方法につきまして以下にご案内致します。
併せて、本脆弱性への対策も含めたセキュリティ強化プログラムを【2017 年 3 月 31 日】にリリースしておりますことをご報告致します。

影響を受けるシステム

ASSETBASE Ver.8.0 およびそれ以前（※）
※現時点での最新バージョンは Ver.8.0 となりますので、提供中の全てのシステムが対象となります。

脆弱性の説明

ASSETBASE の管理者ポータルサイトにクロスサイトスクリプティングの脆弱性が存在します。

想定される影響

ASSETBASE に管理者としてログインしているユーザのウェブブラウザ上で、任意のスクリプトを実行される可能性があります。

対策方法

2017 年 3 月 31 日リリースの ASSETBASE セキュリティ強化プログラムの適用が必要となります。

ASSETBASE クラウド型サービスは既に適用を行っており、対策は完了しております。
オンプレミス型でシステムを導入されているお客様には、弊社よりご案内致します。

回避方法

セキュリティ強化プログラムを適用するまでの間、以下の回避方法を実施することで本脆弱性の影響を軽減することが可能です。

- 当該システムにログインした状態で他のウェブサイトにアクセスしない。
- 作業終了後にはすみやかにログオフを行う。

【参考情報】

ウェブブラウザにはクロスサイトスクリプティング（XSS）対策の機能を有するものがあり、その機能により脆弱性の影響を軽減することが可能です。

次のブラウザでは XSS 対策があります。

Microsoft Edge
Google Chrome
Safari
Internet Explorer ※

次のブラウザには XSS 対策がありません。

Mozilla Firefox

※ Internet Explorer は既定値ではインターネットゾーンの XSS フィルターが有効になっています。しかし、ローカルイントラネットゾーンの XSS フィルターの設定は無効になっているため、ASSETBASE サーバがイントラネットゾーンに存在する環境では XSS フィルターを有効にして使用することで脆弱性の影響を軽減することができます。

設定は「インターネットオプション」の「セキュリティ」タブ内「インターネットゾーン」または「ローカルイントラネット」の「レベルのカスタマイズ…」の画面で確認・変更が可能です。「スクリプト」項の「XSS フィルターを有効にする」のチェックボックスで設定を行います。

動作は以下のブラウザの最新版で確認しました。

Microsoft Edge
Internet Explorer 11
Mozilla Firefox 51
Google Chrome 56
Safari 10

謝辞

この脆弱性情報は、京都大学　山崎啓太郎 様からのご報告をもとに JPCERT コーディネーションセンターから指摘を受けたものです。

お問合せ窓口

ASSETBASE サポートデスク
メールアドレス：abinfo@uchida.co.jp

UCHIDA

実績に基づくIT資産管理ソフトウェア
ASSETBASE

Report on ASSETBASE system cross site scripting vulnerability and release of security enhancement program

April 10, 2017

Thank you for using the IT asset management system ASSETBASE.
From the JPCERT Coordination Center, We received an indication of cross site scripting vulnerability that exists in ASSETBASE Ver. 8.0 and earlier systems. We will inform you about the possible impact of this vulnerability and measures and workarounds as follows.
In addition, we will inform you that we are releasing security enhancement program including measures against this vulnerability on March 31, 2017.

Affected system

ASSETBASE Ver. 8.0 and earlier (*)
* Since the latest version at the present time will be Ver. 8.0, all systems under provision will be covered.

Description of vulnerability

A cross site scripting vulnerability exists in ASSETBASE's administrator portal site.

Possible impact

An arbitrary script may be executed on the web browser of the user logged in to ASSETBASE as an administrator.

Countermeasure

Application of ASSETBASE security enhancement program released on March 31, 2017 is required.
The ASSETBASE cloud type service has already been applied, and measures have been completed.
For customers who have installed on-premise type system, we will inform you from our company.

Workaround

The effect of this vulnerability can be mitigated by implementing the following workaround until applying the security enhancement program.
Do not access other websites while logged into the system.
Log off promptly after work is finished.

[Information]

Some web browsers have a function of countermeasures against cross site scripting (XSS), which can reduce the effect of vulnerability.

There is XSS countermeasure in the next browser.
Microsoft Edge
Google Chrome
Safari
Internet Explorer *

There is no XSS countermeasure in the following browsers.
Mozilla Firefox

* Internet Explorer has XSS filter in the Internet zone enabled by default. However, since the setting of the XSS filter in the local intranet zone is disabled, in an environment where the ASSETBASE server is in the intranet zone, you can reduce the effect of vulnerability by enabling XSS filter.
Settings can be checked and changed on the "Internet Zone" or "Local Intranet" "Level Customization ..." in "Security" tab of "Internet Options".
Make the setting in the "Enable XSS Filter" checkbox in the "Script" section.

The operation was confirmed with the latest version of the following browser.
Microsoft Edge
Internet Explorer 11
Mozilla Firefox 51
Google Chrome 56
Safari 10

Acknowledgments

This vulnerability information was received from the JPCERT Coordination Center based on the report from Kyoto University Keitaro Yamasaki.

Contact

ASSETBASE support desk
E-mail: abinfo@uchida.co.jp