IPA Technical Watch

2013 年 1 月 29 日
独立行政法人情報処理推進機構

IPA テクニカルウォッチ：『DOM Based XSS』に関するレポート

～DOM Based XSS に関する脆弱性の届出が急増～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、IPA に届け出られる「DOM Based XSS」の脆弱性に関する届出が 2012 年後半から増加していることを踏まえ、それらの情報を分析して当該脆弱性の概要や対策のポイントをまとめた技術レポート（IPA テクニカルウォッチ 第 13 回）を公開しました。

IPA に多くの届出があるクロスサイト・スクリプティング（XSS）の脆弱性ですが、2012 年第 1 四半期から第 3 四半期の期間では合計 38 件だった「DOM Based XSS」と呼ばれるタイプのクロスサイト・スクリプティングの脆弱性の届出が、第 4 四半期だけで 92 件（第 3 四半期までの件数比約 2.4 倍増）と急増しました。

一般にクロスサイト・スクリプティングは、サーバ側のプログラムに作り込まれてしまう脆弱性ですが、「DOM Based XSS」と呼ばれるクロスサイト・スクリプティングの脆弱性は、ブラウザのプラグインなどのクライアント側のプログラムに作り込まれてしまう場合があるという特徴があります。

「DOM Based XSS」は、JavaScript から動的に HTML を操作しているアプリ全般に注意が必要な脆弱性です。しかし、本脆弱性を解説した資料が少ないことや、類似の届出が急増したことから、IPA では本脆弱性の原因や対策方法が理解されにくい状況にあると考えました。

以上の経緯から、「DOM Based XSS」の脆弱性について解説した資料を公表することにしました。本資料の対象読者は、ウェブサイトの構築や運営に携わる方、および JavaScript による動的な HTML 操作をするアプリの開発者の方々を想定しています。

脆弱性があるコード例と対策のポイントとして、以下の点について紹介・解説しています。本資料が「DOM Based XSS」の脆弱性の理解と対策方針の参考のために活用されることを期待します。

脆弱性があるコード例を 4 つ紹介

- リンク情報を動的に出力する処理に問題がある例（P.11）
- アクセス解析用のタグの設置方法に問題がある例（P.12）
- JavaScript ライブラリに問題がある例（P.12）
- ウェブブブラウザのプラグインに問題がある例（P.13）

対策のポイントを 3 つ紹介

- DOM 操作用のメソッドやプロパティを使用する方法（P.14）
- 文脈に応じてエスケープ処理を施す方法（P.15）
- JavaScript ライブラリの問題の場合は、ライブラリをアップデートする方法（P.15）

■ 本件に関するお問い合わせ先
IPA　技術本部　セキュリティセンター　小林／金野／谷口
Tel: 03-5978-7527　Fax: 03-5978-7518　E-mail: vuln-inq@ipa.go.jp
■ 報道関係からのお問い合わせ先
IPA　戦略企画部　広報グループ　横山／佐々木
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp