2014年1月16日

弊社ホームページ改ざんに関するお詫びとご報告

弊社ホームページの一部において、第三者からの不正アクセスによりサイトが改ざんされていた事が判明いたしました。ご利用頂いておりますユーザの皆さまにおかれましてはご迷惑をお掛けいたしまして、深くお詫び申し上げます。

なお、現在は被害を受けたサーバのセキュリティ強化等の対策は実施済です。また、ご利用ユーザーの皆さまの個人情報流出等は、現在のところ確認されておりません。

■被害対象サイト／コンテンツ

URLサイト　http://www.kadokawa.co.jp/

■改ざん内容とその影響

改ざん期間中、上記URLサイトにて『Infostealer.Torpplar』と呼ばれる不正なプログラムが書き込まれており、以下の脆弱性のいずれかを有しているユーザーの方がサイトを閲覧した場合、このプログラムが自動的に実行されうると報告されております。なお、本件に伴うご利用ユーザー皆さまの個人情報流出等は、現在のところ確認されておりません。

- **Oracle Java SE Runtime Environment に存在するリモートコード実行の脆弱性（CVE-2012-0507）**
- **Microsoft XML コアサービスに存在するリモートコード実行の脆弱性（CVE-2012-1889）**
- **Oracle Java Runtime Environment に存在する複数のリモートコード実行の脆弱性（CVE-2013-0422）**
- **Adobe Flash Player に存在するリモートメモリ破損の脆弱性（CVE-2013-0634）**
- **Oracle Java SE に存在するメモリ破損の脆弱性（CVE-2013-2465）**

（※影響を受けるシステム：Windows 2000, Windows 7, Windows 95, Windows 98, Windows Me, Windows NT, Windows Vista, Windows XP）

■現在把握している改ざんされていた可能性がある期間

2014年1月7日00時49分 ～ 2014年1月8日13時07分

■改ざん検知後の対応

改ざんがあったことの検知後直ちに当該ファイルの削除及び修正を行い、セキュリティの強化対策を施しました。また、他サーバでは同様の問題が発生していないことを確認いたしました。

■改ざんの原因と経緯

当該サーバーに搭載していたシステムに第三者が不正にアクセスし、特定のファイルが改ざんされたことを確認いたしました。不正アクセスの方法や犯人の特定（警察への相談を含む）等の詳細は調査中です。

■ご利用のユーザーの皆さまへのお願い

上記期間中に、上記 URL サイトにアクセスされた可能性があるユーザーの皆さまにおかれましては、誠にお手数ですが、お手持ちのセキュリティソフトを最新の状態にし、上記の不正なプログラムの感染確認・駆除の実施をお願い申し上げます。

本件につきましては、ご迷惑及びご心配をお掛けいたしましたことを重ねて深くお詫び申し上げますと共に、今後はさらに対策・監視を強化し万全を期して運営して参ります。

以上

▼この件に関するお問い合わせはこちらまで

security201401@lab-kadokawa.com