滋賀県警からのサイバーセキュリティに関するお知らせ

偽決済画面を表示するフォームジャッキング攻撃にご注意

サイト管理者向け

インターネットショッピングサイトからの情報漏えい事案が発生しています。

近年、偽の決済画面を表示して、クレジットカード情報を盗み取る手法（フォームジャッキング攻撃）による情報漏えいが多数確認されています。

特に、株式会社イーシーキューブが提供するサイト構築パッケージ「EC-CUBE」には、フォームジャッキング攻撃に影響を及ぼす脆弱性の存在が確認されていますので、「EC-CUBE」を使用されている方はご注意願います。

EC-CUBE とは

ショッピングサイトが簡単に作成できるソフトウエアのことです。多くの企業で採用されています。

EC-CUBE の脆弱性は 2019 年 5 月頃には確認されており、同製品利用者のショッピングサイトから多くの情報が流出したとされています。

イーシーキューブ社からは、無料診断サービスの提供や注意喚起資料、対策方法が公開されています。

（参考）https://www.ec-cube.net/news/detail.php?news_id=348

クレジットカード番号を盗むフォームジャッキング攻撃

最初に偽のクレジットカード情報入力画面を案内して、クレジットカード情報を入力させた後、エラーを表示させます。再度、正規の入力画面を案内して、クレジットカード情報を入力させ取引を完了させます。利用者にとっては取引自体が 1 度エラーとなるものの、サイトから商品が発送されるので、気づきにくい仕組みになっています。

1 正規のサイトで商品購入を行う

2 偽のクレジットカード情報入力画面を表示

3 エラー画面を表示

4 正規のクレジットカード情報入力画面を表示

インターネット上に公開されているソフトウエアは、便利な反面さまざまなリスクがあります。

EC-CUBE に限らず、多くのソフトウエアには何らかの脆弱性が存在しています。

脆弱性などの問題が発見された場合、多くの企業はソフトウエアの修正プログラムを公開するので、ソフトウエアを利用する側は、それらの修正プログラムを迅速に適用する必要があります。

常にソフトウエアが最新の状態になるよう、更新等を定期的に行うことが重要です。

［お知らせ］偽サイトに注意。ショッピングサイトはＵＲＬも確認しましょう。

滋賀県警察本部サイバー犯罪対策課　（代表）077-522-1231