【重要】サイト改ざんによるクレジットカード流出被害が増加しています。

最終更新日：2019/12/24

■必ずご確認いただき、対策をお願いたします。

最近、EC サイトにおいて、決済画面を改ざんされてクレジットカード情報が抜き取られる手法（フォームジャッキング）による被害が日本国内で増加しています。EC-CUBE では特に 2 系をご利用の店舗で被害が複数報告されておりますので、該当バージョンをお使いの店舗様は以下をお読みいただき、必ず対策を行っていただきますようお願いいたします。

参考記事）https://www.nikkei.com/article/DGKKZO43740260V10C19A4TJQ000/

■EC-CUBE で発生している事象と対策に関して

現在、特に EC-CUBE 2 系で発生している事象として、以下のセキュリティ対策が十分に行われていない場合において EC-CUBE のファイルを改ざんされ、攻撃を受ける可能性がございます。

・正しいインストール環境設定
・EC-CUBE の既知の脆弱性修正対策
・利用しているサーバーのセキュリティ対策
・EC サイトの管理画面のセキュリティ対策
・同じ環境に設置されている他の CMS のセキュリティ対策

以下、具体的なチェック項目と対策方法をお読みになり必要な対策をお願いいたします。

ご自身でチェックや対策が行えない場合や、本メールの内容がご理解いただけない場合は、周辺の詳しい方や、サイト構築を担当された方にご相談ください。
周辺にご相談いただける方がいらっしゃらない場合は、全国の EC-CUBE インテグレートパートナーへもご相談いただけます。
本件に関しましては、セキュリティ対策の専門企業である、SHIFT SECURITY（無償診断）・EG セキュアソリューションズ（無償診断）の簡易診断も提供を予定しております。
詳しくは、本メールの「関連リンク」より各リンク先ページをご覧ください。
また、2 系をお使いで 4 系への移行を御検討の方には、EC-CUBE 4 系をクラウド環境で利用できる「ec-cube.co」を半年間無償で提供させていただきますので、ご利用くださいませ。

■対策前の現状確認チェック

まず、既に「改ざん」が行われていないかをご確認ください。
下記のような「改ざん」の疑いが見つかった場合は、直ちにサイトを停止し、詳しい方にご相談ください。

・購入確認画面等に覚えのない JavaScript が設置されていないか
・購入フローのクレジットカード入力画面が不正な URL になっていないか

■具体的なチェック事項と対策方法

1. EC-CUBE の公開されるべきでないディレクトリが公開されてしまっていないか

EC-CUBE の /data ディレクトリや /install といったディレクトリが運用環境で公開されている場合、そこから管理画面へのアクセス情報やバックアップファイル、アップロードした CSV ファイルなどが流出する恐れがあります。

インストール完了後の/install の削除、/data ディレクトリへのアクセス制限を行なってください。

参考）https://nob-log.info/2013/05/25/wrong-installation-eccube-is-dangerous/

/data ディレクトリのアクセス拒否設定については、設定変更方法資料「4. Data ディレクトリへのアクセスを拒否する方法」をご確認ください。

2. 過去 EC-CUBE より発表された脆弱性が修正されているか

過去の脆弱性を突かれてサイト改ざん等、攻撃されるケースが発生しております。お使いの EC-CUBE のバージョンを管理画面よりご確認の上、過去発表された脆弱性のご確認及び、確実に修正されているかをご確認ください。

https://www.ec-cube.net/info/weakness/

3. 管理画面の URL が /admin/ など推測されやすい URL になっていないか

管理画面の URL を変更せず /admin/ のままで運用していた場合、攻撃者が管理画面にアクセスしやすい状況になっておりますので、 早急に変更をお願いします。

EC-CUBE2.11 以降のバージョンでは、管理画面の URL がインストール時やインストール後の管理画面から変更が可能です。

管理画面の URL を変更する方法は、設定変更方法資料「2. 管理画面の URL を変更する方法」をご確認ください。

4. 管理画面へアクセス制限が行われているか

管理画面のログイン画面に外部から容易にアクセスできる状態ですと、パスワードの総当たり攻撃等で、管理画面にログインされる可能性がございます。

特に、管理画面 URL が/admin/で外部からのアクセスもできる状態ですと、攻撃されやすい状態でございますので、早急に管理画面に部外者がアクセスできないよう対策をお願いします。

・IP 制限をかける（外部からは全くアクセスできない状態にする）
・Basic 認証をかける（管理画面にパスワードをかける）

管理画面へのアクセス制限については、設定変更方法資料「3. 管理画面へのアクセス制 限」をご確認ください。

5. 御利用のサーバーや利用している CMS 等のセキュリティが担保されているか
御利用のサーバーの OS やミドルウェアの脆弱性が対応されているか、サーバー管理者にご確認ください。
WordPress や Drupal などの CMS やその他のファイル操作やデータベースへの接続を行うアプリケーションをインストールしている場合は、各アプリケーションやプラグインの脆弱性が対応されていることもあわせてご確認ください。

■ご自身で対策が難しい場合
対策がご自身ではできない場合は、全国のインテグレートパートナーへご相談ください。
全国のインテグレートパートナー：https://www.ec-cube.net/integrate/partner/

■関連リンク
- 設定変更資料: https://www.ec-cube.net/user_data/news/201905/security_setup.pdf
- 対策がご自分ではできない場合のご相談先
  全国のインテグレートパートナー：https://www.ec-cube.net/integrate/partner/
- 簡易セキュリティ診断のご相談先 （無償診断）
  SHIFT SECURITY：https://www.shiftsecurity.jp/eccube.html
  EG セキュアソリューションズ：https://www.eg-secure.co.jp/ec_cube_contact/
- EC-CUBE 最新版へ移行をご検討の方へ
  クラウド版「ec-cube.co」の半年無償提供：https://www.ec-cube.net/product/co/

■最後に
今回の問題解決にあたり、国内最大規模のオープンソースコミュニティ、EC プラットフォームである立場として、関係省庁とも連携をとりながら積極的に情報発信や対策を実施しております。今後も、EC-CUBE をご利用の店舗様、並びにパートナー様が安心して運営、 ビジネスをしていただけるよう、鋭意対応してまいります。

【本件に関するお問い合わせ窓口】
EC-CUBE 公式お問い合せページ
https://www.ec-cube.net/contact/
株式会社イーシーキューブ
電話：06-4795-7506 受付時間：10～12 時/13～17 時
土日・祝日及び年末年始を除く

EC-CUBE 利用店舗セキュリティチェックリスト

1. 利用環境チェックリスト

a. 利用している EC-CUBE のバージョンはわかる　はい　／　いいえ

b. 管理画面の URL は安易に推測されないよう変更している　はい　／　いいえ

c. 管理画面への IP 制限をおこなっている　はい　／　いいえ

d. 管理画面へのアクセスには常に SSL を利用している　はい　／　いいえ

e. /data へのアクセスを拒否している　はい　／　いいえ

f. /install, install.php は削除している　はい　／　いいえ

g. SSL Labs（https://www.ssllabs.com/ssltest/index.html）にて、SSL のランクが B 以上だと表示される　はい　／　いいえ

h. EC-CUBE の脆弱性リストの対応はおこなっている　はい　／　いいえ

i. 利用している他のアプリケーションを含め運用担当者や相談できる委託先がある　はい　／　いいえ

一つでも**「いいえ」**や**「実態がわからないもの」**がある場合は、前述の無料診断を受けていただくか、既存のご相談先もしくはインテグレートパートナーに御相談ください。

2. サイト改ざんチェックリスト

a. 購入確認画面、カート、購入完了画面に覚えのない JavaScript がある　はい　／　いいえ

b. リンク型決済を利用している場合に、リンク先の URL が契約している決済代行サービスの URL と違っている　はい　／　いいえ

c. サーバーに覚えのないページやファイルがある　はい　／　いいえ

一つでも、**「はい」**や**「実態がわからないもの」**がある場合は、一度サイトを停止して、無料診断を受けていただくか、既存のご相談先もしくはインテグレートパートナーに御相談ください。