滋賀県警察サイバーセキュリティ情報
サイバーコネクトSHIG@
R５年度 No. 7
今、注目のサイバーセキュリティに関する情報をお届けします。

acmailer(エーシーメーラー)の脆弱性に関する注意喚起

今回は、エクストライノベーション株式会社提供のメール配信システム「acmailer」を導入されている事業者様への注意喚起情報です。

当県警に「acmailer」の脆弱性を悪用したサイバー犯罪が実行されているとの情報提供がありました。調査の結果、「acmailer」の管理者権限を取得し、サイバー犯罪の踏み台として利用される実態が浮かび上がりました。

「acmailer」を利用されている事業者様は、最新バージョンにアップデートするなどの措置を取っていただきますよう、よろしくお願いします。

acmailerとは？

「acmailer」は、前述のとおり、エクストライノベージョン株式会社が提供しているメール配信システムで、クラウド型と異なり、自社サーバにインストールして使用するタイプのCGI型システムです。

「acmailer」の特徴は、無料のプランでも顧客条件を絞った配信ができる、スロー配信機能でサーバに負担をかけずに配信ができる、到達率が高い、空メール送信だけでメルマガ登録ができる、といった機能があり、自社でサーバを準備する必要があるものの、あまり費用をかけずに多機能なメール配信システムを構築できるとして、一定の支持を得ています。

～ 脆弱性その１ ～ CVE-2021-20617

○ 脆弱性による影響
　ログインID及びパスワードの上書き
○ 対象バージョン
　acmailer ver 4.0.1以前
　acmailer DB版 ver1.1.3以前
○ 修正方法
　１ バージョンアップする。
　２ バージョンアップが難しい場合は、「init_ctl.cgi」ファイルを削除する。
○ 不正アクセスの確認方法
　「init_ctl.cgi」に対する不審なアクセスログを確認する。インストール時以外に複数回「init_ctl.cgi」に対するアクセスがある場合は、登録情報が漏洩している可能性がある。

～ 脆弱性その２ ～ CVE-2021-20618

○ 脆弱性による影響
　・ acmailer全権限の取得
　・ メールリスト、ログインID、パスワードなどの設定情報の漏洩
　・ cgiファイルの破壊
○ 対象バージョン
　acmailer ver 4.0.2以前
　acmailer DB版 ver1.1.4以前
○ 修正方法
　同脆弱性は、アンケート機能(現バージョンでは不使用機能)に起因するものであるので、バージョンアップではなく、該当ファイルの削除で対応可能。
　「enq_detail.cgi」、「enq_detail_mail.cgi」、「enq_edit.cgi」、「enq_form.cgi」、「enq_list.cgi」の５つのファイルを削除する。

～ 脆弱性その３ ～

○ 脆弱性による影響
　第三者から任意のコマンドを実行される。
○ 対象バージョン
　acmailer ver 4.0.3以前
　acmailer DB版 ver1.1.5以前
○ 修正方法
　バージョンアップする。

それぞれの脆弱性情報の詳細は、acmailerのWebページ https://www.acmailer.jp/info/index.cgi を参照してください。

**滋賀県警察
サイバー犯罪対策課
【公式】Twitter
始めました！**