



acmailer (エ-シー-メ-ラ-) を最新のバージョンにアップデートしてください。

～脆弱性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、登録情報が漏えいしている可能性があります。



～脆弱性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
- 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ため、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
- 修正方法
バージョンアップする。



バージョン4.0.3以前（DB版1.1.5以前）は危険!!
必ずバージョンアップをしてください。



一斉送信メールや、メールマガジンの配信で利用される、acmailer (エ-シー-メ-ラ-) というメール配信システムには脆弱性があり、バージョンアップ等の対策をしないと、犯行予告等の踏み台とされたり、個人情報などが漏えいする被害に遭うおそれがあります。

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。



長野県警察公式ホームページの「サイバーセキュリティ対策」には、サイバー事案等の手口や被害に遭わないための情報が掲載されています。是非ご覧ください。