



acmailerを最新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、登録情報が漏れ
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。

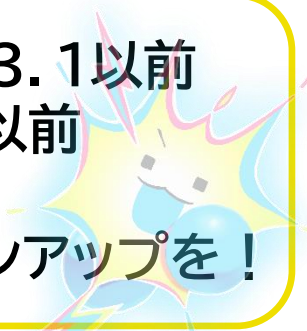


～脆弱性③～

- 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4.3.1以前
DB版1.1.5以前
は危険！！
必ずバージョンアップを！



一斉送信メールやメールマガジンの配信で利用されるメール配信システム「acmailer」には、脆弱性があり、バージョンアップをしないと、乗っ取られて、悪用されるリスクがあります。

詳細は、acmailerのWebページを参照してください。↓↓
<https://www.acmailer.jp/info/index.cgi>

