* 1. 発見した脆弱性詳細

1. バッファオーバーフロー

* 危険度

Low

* 解説

バッファ（データの一時記憶領域）に、想定以上の長さのデータが入力されてしまい、システムの停止につながる現象。

▼再現方法

ログイン画面のテキストボックスの値を以下のように操作する。

ユーザID欄やパスワード欄に大量の文字列を打ち込む（500文字で実行）

上記の通り操作したところ、次のようにエラーメッセージが出力されたことから、汎用エラーが発生しており、バッファオーバーフローに脆弱であると判断できる。

[出力されたエラーメッセージ]

Error: Request failed with status code 500

* 想定される被害・影響

・データベースサーバーシステムが停止する。

・実行中のプログラムが強制終了してしまう。

* 対策

・バリデーション（入力の検証）：データのサイズや書式などが想定どおりになっていることを確認する。

・サニタイジング（無害化）：データ内に危険なコードなどが含まれていたら実行不能な状態にする

* 備考

特になし。