文書番号：PBSP-20083

遠隔監視制御システム
コルソス CSDJ お客様各位

2021 年 2 月 15 日

NEC プラットフォームズ株式会社
パブリックシステム事業部
営業推進本部

コルソス CSDJ シリーズにおける脆弱性について

1. 概要

コルソス CSDJ において、脆弱性が存在することが判明しました。この脆弱性に対して悪意ある第三者から攻撃された場合、ユーザーが権限を与えられていない履歴にアクセス可能となる危険性があります。

つきましては、５項の対策方法、または、６項の回避策を実行されますようお願いいたします。

2. 対象製品

品名	対象バージョン	出荷時期
CSDJ-B/H/D	01.08.00 以前	2021 年 3 月以前の出荷品（※）
CSDJ-A	03.08.00 以前	

※出荷時期は参考情報になります。対象製品かどうかはバージョンをご確認ください。

コルソス CSDJ のバージョンの確認方法は、以下の通りです。

1. パソコンからコルソスにアクセスし、ブラウザコントロールでログインします。
2. ログイン後、[その他]->[バージョン情報]を選択し、「FW バージョン」に表示されている部分がコルソス CSDJ のバージョン番号です。

詳細な手順については、CSDJ 総合説明書を参照してください。

3. 脆弱性の説明

コルソス CSDJ には、ブラウザコントロール上で、端末の履歴を表示する機能があり、その表示内容については、管理者がユーザーごとに履歴閲覧権限を割り当てることができます。しかし、悪意ある権限のないユーザーが、意図的な改ざんを行った場合、権限のないユーザーであっても履歴を閲覧できてしまう可能性があります。

※コルソス CSDJ の履歴には、「ログイン履歴」、「動作履歴」、「コントロール履歴」、「通報履歴」があります。

4. 脆弱性がもたらす脅威

コルソス CSDJ の履歴の閲覧を許可されていないユーザーであっても、履歴が閲覧可能となる可能性があります。

5. 対策方法

当社にて、脆弱性の対策を致しました。ファームウェアのアップデートをお願いします。

<CSDJ-B/H/D>

・ファームウェアのダウンロード先

https://www.necplatforms.co.jp/product/enkaku/csdj/fw_requirement.html

（2021 年 2 月 15 日よりダウンロード可能）

・ファームウェアのアップデート方法

総合説明書「工事編」の「ファームウェア・アップデート」に従って実施してください。

<CSDJ-A>

・ファームウェアのダウンロード先

https://www.necplatforms.co.jp/solution/i-iot/csdj-a/fw_requirement.html

（2021 年 2 月 15 日よりダウンロード可能）

・ファームウェアのアップデート方法

総合説明書「工事編」の「ファームウェア・アップデート」に従って実施してください。

6. 回避策

前項の対策方法を行うことが難しい場合、ユーザーにすべての履歴の閲覧権限を与えなければ、この脆弱性を回避することができます。（「ログイン履歴」、「動作履歴」、「コントロール履歴」、「通報履歴」のどれか 1 つでもユーザーに閲覧権限がある場合に、この脆弱性が発生します。）

7. 関連情報

脆弱性識別番号：JVN#87164507

8. 謝辞

本脆弱性の発見者である 横浜国立大学 佐々木貴之 様、吉岡克成 様に厚く御礼申し上げます。
（届出者情報順）

9. 更新履歴

2021/02/15：この脆弱性情報を公開しました。

10. 連絡先

コルソス CSDJ の脆弱性に関する問い合わせ窓口（2021 年 2 月 15 日～2021 年 8 月 31 日）
メール：security_info@calsos.jp.nec.com

以上