\Orchestrating a brighter world NEC

文書番号：PB2ITS-18010(2)

遠隔監視制御システム

2018 年 7 月 12 日

コルソス CSDJ / CSDX お客様各位

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 / CSDX シリーズの ブラウザアクセスに関する脆弱性について

1. 概要

コルソス CSDJ / CSDX において、アクセス制限不備などの複数の脆弱性が存在することが判明しました。これらの脆弱性に対して悪意ある第三者から攻撃された場合、運用が停止させられるなどの危険性があります。

つきましては、ネットワークに接続して運用されている場合、４項の対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	01.03.00 以前	2018 年 6 月以前の出荷品
CSDJ-A	03.00.00	
CSDX	1.37210411 以前	全出荷品（2016 年 6 月販売終了）
CSDX(S)	2.37210411 以前	
CSDX(D)	3.37210411 以前	
CSDX(P)	4.37210411 以前	

3. 脆弱性の説明

3.1 脆弱性の内容

コルソス CSDJ / CSDX シリーズは、アクセス制限不備やクロスサイトスクリプティングなど複数の脆弱性が存在します。

・アクセス制限不備

ブラウザコントロール機能において、管理者権限のないユーザーにより、任意の管理者権限の操作が実行される可能性があります。

・クロスサイトスクリプティング

当該製品にログインしているユーザーのウェブブラウザ上で、任意のスクリプトを実行される可能性があります。

3.2 脆弱性がもたらす脅威

コルソスはブラウザコントロールにて、システムデータの変更や出力制御などの機能を提供していますが、これら機能の悪用による脅威が考えられます。

・システムデータを無効な値に変更したり、初期化したりすることで、運用停止される可能性があります。

・システムデータの値を変更することで、意図しない運用状態に変更される可能性があります。

・デジタル / アナログ出力を制御することで、外部機器、設備の意図しない動作が実行される可能性があります。

・センサーなどのログデータが流出したり、消去されたりする可能性があります。

3.3 運用形態による危険性の差異

コルソスの脆弱性は、ブラウザアクセスしている場合に問題となるものです。ネットワークに接続せず運用されている場合には影響ありません。

ネットワークの運用により、危険性が変わります。

<危険性のある運用>

ネットワークに接続しており、不特定多数からコルソスにアクセスできる状態での運用。

<危険性の少ない運用>

ネットワークに接続される運用においても、以下の場合は、危険性は少なくなります。

・外部のネットワークに接続していない（閉域網で使用している）場合

・ファイアウォールなどを使用して、

・外部からコルソスへのアクセスができない場合

・外部からコルソスへのアクセスが特定のユーザーに限定している場合

・ダイヤルアップで接続する場合

4. 対策方法

4.1 ファームウェアアップデート

これらの脆弱性を解消したファームウェアを提供しますので、脆弱性対策されたファームウェアにアップデートしてください。

<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

（2018 年 7 月 2 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 に関しては別途お問い合わせください。

<CSDX>

・ファームウェアのダウンロード先

https://www.necplatforms.co.jp/product/enkaku/login.html

（2018 年 7 月 2 日よりダウンロード可能）

・ソフトウェアのアップデート方法

修正プログラムに添付されている資料に従って実施してください。

4.2 環境設定

これらの脆弱性は、外部からのアクセスを制限することで影響を緩和できる場合があります。

<コルソス側での対策>

・ID、パスワードの変更および管理強化

・利用ユーザーの限定

<ネットワーク側の対策>

・ルーター、ファイアウォールの設定（設置）

・外部からのアクセスを拒否する

または、

・外部からのアクセス元を限定する

5. 関連情報

公開サイト：　https://www.necplatforms.co.jp/product/enkaku/info180702.html

6. 更新履歴

2018 年 7 月 2 日：この脆弱性情報を公開しました。

2018 年 7 月 2 日：<CSDJ-B/H/D>ファームウェアのダウンロード先を変更しました。

7. 連絡先

コルソス脆弱性コールセンター（2018 年 7 月 2 日 ～ 2018 年 12 月 28 日）

電話：0120-304414　（土日祝日当社夏季休暇除く 9:00 ～ 17:00）

スマートアクセスソリューション営業推進部

電話：03-5282-5842　（土日祝日当社休暇除く 9:00 ～ 17:00）

メール：info@enkaku.jp.nec.com

以上