【重要なお知らせ】HIKVISION 製レコーダーの重要なセキュリティ情報について

平素は格別のご高配を賜り厚く御礼申し上げます。

このたび HIKVISION 製のレコーダー一部の機種において OSD 画面に以下のメッセージが表示される現象が複数確認されました。

- 「your CCTV is vulnerable and can be exposed」

HIKVISION 社に確認した結果、現時点で公開されていない製品の脆弱性によるトラブルではないとのことです。

運用方法によっては、同様の現象が生じる可能性がございますので、該当製品をご利用頂いておりますお客様におかれましては、ご注意の上、ご使用いただきますようご案内致いたします。

■ 現象の発生原因：ネットワーク、パスワード認証方式の脆弱性を利用したアクセスによるもの

- 遠隔接続のためにネットワーク環境の変更及びデフォルトや予測されやすいパスワードを利用することによって発生する可能性が高いことが確認されています。

■ 対象：HIKVISION 製レコーダー(機種や F/W の規則性無し)
現時点で症状が確認されている機種：DS-7604NI-K1 / 4P(B)、iDS-7204HUHI-M1 / P、DS-7608NI-K2/8P、DS-7604NI-I1/4P

■ 現象が発生する可能性がある運用方法：

① DDNS(dynamic domain name system)もしくは固定 Global IP をご使用中の場合
② 遠隔監視のためにルーターのポートを開放している場合
③ 初期パスワードだけではなく、予測可能なパスワードを使用している場合(例に関しては添付を参照)

■ 上記の運用方法がセキュリティレベルが低いとされる理由

① 外部からの接続をする場合に必要な情報は以下の 3 つになります。
Global IP アドレス、ポート番号、本体の ID / PW
② ポート開放による接続方式は遠隔接続するための 3 つの情報が取得しやすいため、セキュリティレベルが低いといえます。
③ さらにサイバー攻撃の 5 割以上は Web ポートによって発生しますので、Web ポートを開けていて、さらにパスワードが予測されやすいと攻撃されやすいです。

上記の運用方法で製品をご使用されている代理店様は、以下の対策を行って下さい。

1. パスワードの変更

- 適切なセキュリティレベルのパスワードに変更してください。 ユーザー専用かつ予測されにくい難しいパスワードに変更していただければと思います
例えば大文字、英数字の組み合わせ、特殊文字を含むパスワードがおすすめです。

2. ローカルネットワークでの運用

- 可能であれば、レコーダーをローカルネットワーク上で運用してください。
外部からのアクセスを制限でき、セキュリティリスクを低減することができます。
遠隔監視を行う場合は以下の 3 番の方法で接続を推奨します。

※ 現場環境や特定の目的で DDNS や Global IP とポート開放の組み合わせで運用される場合は Web ポートを開けないことでリスクを少しでも減らすことができます。
もしくは UTM(Unified Threat Management)デバイスを導入し、ポートや ID/PW を探るための不正なアクセスを防ぐことを推奨いたします(弊社 UTM 紹介ページ)

3.遠隔監視には VPN 構成や HIK-Connect を使用する

- VPN を使用する場合、セキュリティ、プライバシーが強化され、データーを暗号化しており、外部からアクセスが困難になるため有効です。
- HIK-Connect の場合、P2P 通信方式で HIK Server より Global IP, Port 情報を確認、管理していて、その情報にアクセスするためには HIK-Connect の ID/PW が分かっているもしくは HIK のサーバーをハッキングしないといけないため、セキュリティが高いです。

4. F/W が古い場合は最新 F/W に Update する - 手順書参照

①F/W Update する。(Update 後は初期化することを推奨)
②再度デバイスを Activate

※F/W Update はセキュリティ強化に役を立ちますが、本件には直接影響はありません。
以上の対策を行うことで、セキュリティリスクを軽減することができます。

ご案内させていただいた対策は予防の対策になっており、既にメッセージが表示されてしまう場合、カメラの OSD メニューからメッセージを削除することも可能です。以下の手順にて設定変更を行ってください。(詳細はマニュアルを参照)

① 設定-画像-OSD 設定-テキストオーバーレイを選択
② 削除したいテキストを選択し、保存
③ ルーターのポートは変更することを推奨

弊社は、製品の脆弱性に関する情報収集を継続しており、最新の情報に基づき、お客様に適切な対策を提供してまいります。
ご質問やご不明点がございましたら、お気軽にお問い合わせください。

株式会社セキュリティデザイン