お知らせ

NIS-Elements 製品における AVI および Mpeg 形式の動画ファイルやストリーミング機能に影響する複数の脆弱性修正について

掲載日　2024 年 12 月 11 日

株式会社ニコン　ヘルスケア事業部

1．概要

NIS-Elements 製品において、AVI および Mpeg 形式の動画ファイルやストリーミング機能に影響する複数の脆弱性を修正しました。

2．該当製品と確認方法

本問題の影響を受ける該当製品とバージョンは以下のとおりです。

製品名	バージョン
NIS-Elements Advanced Research	Ver.6.10.00A 迄の全バージョン
NIS-Elements Basic Research	Ver.6.10.00A 迄の全バージョン
NIS-Elements Documentation	Ver.6.10.00 迄の全バージョン
NIS-Elements Confocal	Ver.6.10.00A 迄の全バージョン
NIS-Elements Enhanced Resolution	Ver.6.10.00A 迄の全バージョン
NIS-Elements L	Ver.1.22 迄の全バージョン

バージョン番号は、以下の何れかの方法で確認できます。

1)メニューから[Help] > [About]を選択するとバージョン番号が確認できます。

2)NIS-Elements AR/BR/D や L のリリースノート内のタイトルからでもバージョン番号が確認できます。

```
////////////////////////////////////////////////////////////////////////////////
          NIS-Elements Advanced Research Ver.6.10.00A
          NIS-Elements Basic Research Ver.6.10.00A
          Copyright(C) 2024 Nikon Corporation All rights reserved.
////////////////////////////////////////////////////////////////////////////////
```

3．対策済脆弱性

1)FFmpeg.exe を n7.1 に更新しました

2)修正された主な脆弱性は下表のとおりです

脆弱性カテゴリー	脆弱性の影響	CVE 番号	影響する機能
バッファオーバーリード	悪意あるコード実行	CVE-2022-3964	AVI および Mpeg 形式動画ファイルやストリーミング機能に影響しております
ヒープベースのバッファオーバーフロー	悪意あるコード実行	CVE-2024-7055 CVE-2022-2566	
バッファオーバーライト	悪意あるコード実行	CVE-2024-7272	

3)詳細情報

修正された脆弱性の詳細情報については、FFmpeg の公式サイト(FFmpeg Security)から確認する事ができます。

４．脆弱性がもたらす脅威

攻撃者によって細工された画像ファイルを開くことで、任意のコードが実行される可能性があります。

５．対策方法

対策方法は、以下の通りです。

製品名	対策
NIS-Elements Advanced Research	Ver.6.10.00B 以降にアップデートしてください
NIS-Elements Basic Research	Ver.6.10.00B 以降にアップデートしてください
NIS-Elements Documentation	Ver.6.10.00B 以降にアップデートしてください
NIS-Elements Confocal	Ver.6.10.00B 以降にアップデートしてください
NIS-Elements Enhanced Resolution	Ver.6.10.00B 以降にアップデートしてください
NIS-Elements L	Ver.1.22.00A 以降にアップデートしてください

ソフトウェアは以下の URL からダウンロードして下さい。

https://www.microscope.healthcare.nikon.com/ja_JP/software-firmware

６．軽減策・回避策

すぐに製品をバージョンアップできない場合には、次の軽減策を推奨します。

・信頼できないファイルを開かない。

7. お問い合わせ先

担当営業にお問い合わせください
