

お知らせ

NIS-Elements Ver.5.4x 製品における複数の脆弱性修正について

掲載日 2024年12月27日

株式会社ニコン ヘルスケア事業部

1. 概要

NIS-Elements Ver.5.4x 製品において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.5.42.06 迄の全バージョン
NIS-Elements Basic Research	Ver.5.42.06 迄の全バージョン
NIS-Elements Documentation	Ver.5.42.06 迄の全バージョン
NIS-Elements Confocal	Ver.5.42.06 迄の全バージョン
NIS-Elements Enhanced Resolution	Ver.5.42.06 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。

3. 対策済脆弱性

3.1. NIS-Elements Ver.5.4x 製品において画像ファイル読み込み時の複数の脆弱性を修正しました。

対策した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	対象画像ファイル
バッファオーバーリード	悪意あるコード実行	CVE-2022-40656	ND2 ファイル
		CVE-2022-40662	TIFF ファイル
		CVE-2022-40663	TIFF ファイル
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-2022-40661	BMP ファイル
		CVE-2022-40660	PSD ファイル
		CVE-2022-40655	ND2 ファイル
バッファオーバーライト	悪意あるコード実行	CVE-2022-40657	PSD ファイル
		CVE-2022-40658	TIFF ファイル
		CVE-2022-40659	TIFF ファイル

3.2. NIS-Elements Ver.5.4x 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。

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](#)) から確認することができます。

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.5.42.07 にアップデートしてください
NIS-Elements Basic Research	Ver.5.42.07 にアップデートしてください
NIS-Elements Documentation	Ver.5.42.07 にアップデートしてください
NIS-Elements Confocal	Ver.5.42.07 にアップデートしてください
NIS-Elements Enhanced Resolution	Ver.5.42.07 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

こちらに掲載されている情報は、発表日現在の情報です。販売が既に終了している製品や、組織の変更等、最新の情報と異なる場合がありますのでご了承ください。