

Notification
Fixed Vulnerabilities in NIS-Elements Ver.5.4x Products.

Updated on August 1, 2025.
Healthcare Business Unit
NIKON CORPORATION

1. Overview

The information in section "6. Mitigation and Workarounds" has been updated in the previously announced notice, "Fixed Vulnerabilities in NIS-Elements Ver.5.4x Products" (published on December 27, 2024).

2. Affected products and how to check

The affected products and versions are as follows:

Product Name	Version
NIS-Elements Advanced Research	All versions up to Ver.5.42.06.
NIS-Elements Basic Research	All versions up to Ver.5.42.06.
NIS-Elements Documentation	All versions up to Ver.5.42.06.
NIS-Elements Confocal	All versions up to Ver.5.42.06.
NIS-Elements Enhanced Resolution	All versions up to Ver.5.42.06.

You can check the version number using one of the following methods:

- 1) Select [Help] > [About] from the menu to view the version number.

3. Fixed Vulnerabilities

3.1. Fixed Vulnerabilities when image reading in NIS-Elements Ver5.4x Products.

The following vulnerabilities has been fixed.

Vulnerability Category	Vulnerability Impact	CVE-ID	Affected Image Files
out-of-bounds read	execute malicious code	CVE-2022-40656	ND2 file
		CVE-2022-40662	TIFF file
		CVE-2022-40663	TIFF file
heap-based buffer overflow	execute malicious code	CVE-2022-40661	BMP file
		CVE-2022-40660	PSD file
		CVE-2022-40655	ND2 file
out-of-bounds write	execute malicious code	CVE-2022-40657	PSD file
		CVE-2022-40658	TIFF file
		CVE-2022-40659	TIFF file

3.2. Fixed Vulnerabilities affecting AVI and MPEG video files and streaming function in NIS-Elements Ver.5.4x Products.

1) Updated FFmpeg.exe to n7.1

2) The main vulnerabilities that have been fixed are as follows:

Vulnerability Category	Vulnerability Impact	CVE Numbers	Affected features
out-of-bounds read	execute malicious code	CVE-2022-3964	Affects AVI and MPEG video files and streaming functionality
heap-based buffer overflow	execute malicious code	CVE-2024-7055 CVE-2022-2566	
out-of-bounds write	execute malicious code	CVE-2024-7272	

3) Detailed information

Detailed information about the fixed vulnerabilities can be found on the FFmpeg official website ([FFmpeg Security](#)).

4. Threats posed by the vulnerabilities

Opening an attacker-crafted image files may allow arbitrary code to be executed.

5. Countermeasures

The countermeasures are as follows:

Product Name	countermeasure
NIS-Elements Advanced Research	Please update to Ver.5.42.07.
NIS-Elements Basic Research	Please update to Ver.5.42.07.
NIS-Elements Documentation	Please update to Ver.5.42.07.
NIS-Elements Confocal	Please update to Ver.5.42.07.
NIS-Elements Enhanced Resolution	Please update to Ver.5.42.07.

Please download the software from the following URL.

[Europe and Asia Region]

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

[Americas Region]

<https://www.nissoftware.net/NikonSaleApplication/>

6. Mitigation and Workarounds

If immediate product version upgrade is not possible, the following mitigation measures and workarounds are recommended:

- Do not open untrusted files.
- Install NISFileChecker and Shell Extension. (Added on June 30, 2025)

For customers using NIS-Elements products from Ver.5.00.00 to Ver.5.42.06 who are unable to upgrade to NIS-Elements Ver.5.42.07 or later, the vulnerabilities described in section 3.1 can be avoided by using the following software:

- | | |
|--------------------|---|
| • NISFileChecker: | Application for image file checking |
| • Shell Extension: | Extension application for thumbnail display |

These software applications can be downloaded from the following URL.

[Europe and Asia Region]

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

[Americas Region]

<https://www.nisoftware.net/NikonSaleApplication/>

Please note that the vulnerabilities described in section 3.2 are not addressed by NISFileChecker or Shell Extension.

7. Contact Information

Please contact your sales representative

The information posted here is current as of the date of announcement. Please note that the information may differ from the latest information, such as products that are no longer on sale or organizational changes.