Notification
Fixed Vulnerabilities affecting AVI and MPEG video files and streaming function in NIS-Elements Products.

Published on December 11, 2024.
Healthcare Business Unit
NIKON CORPORATION

1. Overview

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

2. Affected products and how to check

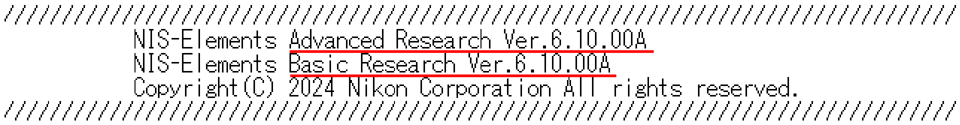
The affected products and versions are as follows:

Product Name	Version
NIS-Elements Advanced Research	All versions up to Ver.6.10.00A
NIS-Elements Basic Research	All versions up to Ver.6.10.00A
NIS-Elements Documentation	All versions up to Ver.6.10.00
NIS-Elements Confocal	All versions up to Ver.6.10.00A
NIS-Elements Enhanced Resolution	All versions up to Ver.6.10.00A
NIS-Elements L	All versions up to Ver.1.22

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

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

2) You can also find the version number in the title of the release notes for NIS-Elements AR/BR/D or L.



```
////////////////////////////////////////////////////////////////////////////////
            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．Fixed Vulnerabilities

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.6.10.00B or later.
NIS-Elements Basic Research	Please update to Ver.6.10.00B or later.
NIS-Elements Documentation	Please update to Ver.6.10.00B or later.
NIS-Elements Confocal	Please update to Ver.6.10.00B or later.
NIS-Elements Enhanced Resolution	Please update to Ver.6.10.00B or later.
NIS-Elements L	Please update to Ver.1.22.00A or later.

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.nisoftware.net/NikonSaleApplication/

6． How to reduce/avoid the threat

If you are unable to upgrade your product immediately, we recommend the following mitigation measures:

・Do not open untrusted files.

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.