Notification
Fixed Vulnerabilities When Image Reading in NIS-Elements Products.

Published on August 29, 2024
Healthcare Business Unit
NIKON CORPORATION

1． Overview

Vulnerabilities has been Fixed in NIS-Elements Products when reading image files.

2． How to check if your software affected:

The affected products and version are as follows:

Product name	Version
NIS-Elements Advanced Research	Ver.6.02.03 and earlier
NIS-Elements Basic Research	Ver.6.02.00 and earlier
NIS-Elements Documentation	Ver.6.02.00 and earlier
NIS-Elements Confocal	Ver.6.02.03 and earlier
NIS-Elements Enhanced Resolution	Ver.6.02.03 and earlier

To check your software's version, refer to the steps below:

Go to Menu and select [Help] > [About], The Version information dialog box will open.

3． Fixed Vulnerabilities

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 CVE-2022-40662 CVE-2022-40663	ND2 file TIFF file TIFF file
heap-based buffer overflow	execute malicious code	CVE-2022-40661 CVE-2022-40660 CVE-2022-40655	BMP file PSD file ND2 file
out-of-bounds write	execute malicious code	CVE-2022-40657 CVE-2022-40658 CVE-2022-40659	PSD file TIFF file TIFF file

4． Threats posed by the vulnerabilities

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

5． Countermeasure

The countermeasure is as follows:

Product name	Version
NIS-Elements Advanced Research	Update the software to Ver.6.10.00 or later.
NIS-Elements Basic Research	Update the software to Ver.6.10.00 or later.
NIS-Elements Documentation	Update the software to Ver.6.10.00 or later.
NIS-Elements Confocal	Update the software to Ver.6.10.00 or later.
NIS-Elements Enhanced Resolution	Update the software to Ver.6.10.00 or later.

Please download the software from the following URL:

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

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 is current as of the date of publication. It is subject to change without notice.