Vulnerabilities found in KV STUDIO and KV REPLAY VIEWER functions

Published on March 29, 2024
KEYENCE CORPORATION

■ Overview

The following vulnerabilities have been found in KV STUDIO and KV REPLAY VIEWER:

· Out-of-bounds read

· Out-of-bounds write

The affected versions of KV STUDIO and KV REPLAY VIEWER are listed below.

■ How to check if your software is affected:

The affected products and versions are as follows:

Product name	Version
KV STUDIO	Ver.11.64 and earlier
KV REPLAY VIEWER	Ver.2.64 and earlier

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

Go to Menu and select Help > Version information. The Version information dialogue box will open.

■ Description of the vulnerabilities

The affected products contain out-of-bounds read and out-of-bounds write vulnerabilities.

■ Threats posed by the vulnerabilities

If a user opens a file that has been maliciously crafted by an attacker, arbitrary code may be executed.

■ Countermeasures

The countermeasures are as follows:

Product name	Countermeasure
KV STUDIO	Update the software to Ver.11.65 or later.
KV REPLAY VIEWER	Update the software to Ver.2.65 or later.

■ How to reduce/avoid the threat

If you are unable to update your software immediately, we recommend that you take the following mitigation measures:

· Do not open any untrusted files.

· Install anti-virus software on PCs on which you use the software.

■ Acknowledgment

We express our gratitude to Mr. Michael Heinzl for reporting the vulnerabilities.

■ Contact information

Please contact your nearest KEYENCE office.

Copyright © 2024 KEYENCE CORPORATION. All rights reserved.