KSR-PSIRT-Q005
Published on October 18, 2022
Last updated on October 18, 2022

KSR-PSIRT-Q005: Vulnerability in YOKOGAWA application software WTViewerE

■Overview**:**

A vulnerability has been found in YOKOGAWA application software. The products that may be affected by this vulnerability are listed below.

Review this report and confirm which products are affected to implement security measures for the overall systems. Please consider applying the countermeasures as needed.

■**Affected Product**:

- WTViewerE 761941
- WTViewerEfree

■Vulnerability:

A stack-based buffer overflow vulnerability exists when saving a file containing a long filename. An attacker could exploit this vulnerability to execute code in the context of the current process.

The following countermeasures (putting a restriction on long filenames) can prevent the vulnerability.

■Countermeasures:

Product	Description	Affected version	Fixed version	Countermeasure
WTViewerE 761941	To resolve a vulnerability in file save function.	1.31-1.61	1.62	Please update to 1.62 from the link *1 shown below.
WTViewerEfree	To resolve a vulnerability in file save function.	1.01-1.52	1.53	Please update to 1.53 from the link *2 shown below.

*1:
https://tmi.yokogawa.com/jp/library/documents-downloads/software/761941-wtviewere-upgrade-version/

*2: http://tmi.yokogawa.com/jp/library/documents-downloads/software/wtviewerefree_software/

If you need assistance with the update, please contact our customer support.

We strongly recommend all customers establish and maintain a full security program, not only for the vulnerability identified in this Security Advisory Report. Security program components include patch updates, anti-virus, backup and recovery, zoning, hardening, whitelisting, firewall, and so on.

KSR-PSIRT-Q005
Published on October 18, 2022
Last updated on October 18, 2022

■Contact:

- Contact the customer support from https://tmi.yokogawa.com/contact/technical-and-service-support/