KW Watcher Vulnerability Allowing Malicious Memory Read Access

Date of announcement: April 22, 2024

Panasonic Industry Co., Ltd.

■Overview

A vulnerability that could permit malicious memory read access has been found in KW Watcher. Opening a malicious KWW file could give an attacker read access to memory.

■Affected product

Name	Software version
KW Watcher	All versions

■CVSS score

CVSS: 3.1 / AV: L / AC: L / PR: N / UI: R / S: U / C: L / I: N / A: L Base score: 4.4

■Description of vulnerability

A buffer error (CWE-119) in KW Watcher has caused a vulnerability that could allow malicious read access to memory.

■Threat from vulnerability

An attacker might be able to exploit this vulnerability to infer information about a computer’s memory map.

■Countermeasures

Please take steps to reduce or avoid the risks posed by this vulnerability.

■Steps to reduce or avoid risks

The following steps are recommended in order to minimize the risks posed by this vulnerability:

- Do not open KWW files of unknown provenance.
- If opening a KWW file causes a dialog describing an error such as a “File open error” to be displayed or KW Watcher to terminate abruptly, please stop using the file in question.

■Acknowledgment

Panasonic wishes to thank Michael Heinzl for reporting this vulnerability.