24-R&D-0219

WindLDR and WindO/I-NV4 store sensitive information in cleartext

IDEC Corporation

Published date: August 29, 2024

Overview

It has been discovered that our PLC programming software WindLDR and Operator Interfaces' Touchscreen Programming Software WindO/I-NV4 contain a vulnerability in which sensitive information may be stored in cleartext form (CWE-312). An attacker who obtains a project file could obtain user authentication information for the PLC or Operator Interfaces and potentially operate the PLC or Operator Interfaces illegally.

CVSS

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score: 5.9

Affected products

The following products and software versions are affected.

Product name	Software version
WindLDR	Ver.9.1.0 and earlier
WindO/I-NV4	Ver.3.0.1 and earlier

Description of vulnerabilities

The project files saved by WindLDR and WindO/I-NV4 do not have sufficient file protection, which may allow important information such as authentication information to be stolen.

Impact

An attacker who obtains a project file could obtain authentication information for the PLC or Operator Interfaces and potentially operate the PLC or Operator Interfaces illegally.

Countermeasures for Customers

The fixed products and software versions are as follows.

Product name	Software version
WindLDR	Ver.9.2.0 and later
WindO/I-NV4	Ver.3.1.0 and later

Please download the latest version of each software from our website and update it.

Mitigations/Workarounds

Please properly manage project files saved by WindLDR and WindO/I-NV4 to prevent them from being leaked.

Update history

This vulnerability information page was published on August 29, 2024.

Credit

Yuki Meguro of Toinx Co., Ltd. for reported this vulnerability.

Thanks to Yuki Meguro for finding and reporting it

Contact information

Please contact us via our website.