Unprotected Transport of Credentials, Plaintext Storage of a Password

IDEC Corporation

Published date: December 24, 2021

Last update date: December 24, 2021

Overview

It has been discovered that our PLCs and their programming software contain vulnerabilities that may result in the leakage of authentication information due to insufficient protection of authentication information.
An attacker could obtain authentication information from communication data or files created by the programming software and potentially manipulate the PLC. (CVE-2021-37400、CVE-2021-37401、CVE-2021-20826、CVE-2021-20827)

CVSS

CVE-2021-37400 CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L Base Score: 7.6

CVE-2021-37401 CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L Base Score: 7.6

CVE-2021-20826 CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L Base Score: 7.6

CVE-2021-20827 CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L Base Score: 7.6

Affected products

The following products and software versions are affected.

Product name	Software version
FC6A Series MICROSmart All-in-One CPU	2.32 and earlier
FC6B Series MICROSmart All-in-One CPU	2.31 and earlier
FC6A Series MICROSmart Plus CPU	1.91 and earlier
FC6B Series MICROSmart Plus CPU	2.31 and earlier
FT1A Series SmartAXIS Pro/Lite	2.31 and earlier
WindLDR	8.19.1 and earlier
Data File Manager	2.12.1 and earlier
WindEDIT Lite	1.3.1 and earlier

Description of vulnerabilities

Our PLCs and their programming software contain a vulnerability that may allow authentication information to be stolen from the communication data, or files created by the programming software due to insufficient protection of authentication information.

Impact

A malicious attacker could steal authentication information and perform unauthorized operations such as reading or rewriting programs in the PLC.

Countermeasures for Customers

The fixed products and software versions are as follows.

Product name	Software version
FC6A Series MICROSmart All-in-One CPU	2.40 and later
FC6B Series MICROSmart All-in-One CPU	2.40 and later
FC6A Series MICROSmart Plus CPU	2.00 and later
FC6B Series MICROSmart Plus CPU	2.40 and later
FT1A Series SmartAXIS Pro/Lite	2.40 and later
WindLDR	8.20.0 and later
Data File Manager	2.13.0 and later
WindEDIT Lite	1.4.0 and later

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

Mitigations/Workarounds

In order to minimize the risk of these vulnerabilities being exploited, please use a closed network such as a dedicated network or VPN. For details, please refer to the Security Precaution on our website.

Update history

This vulnerability information page was published on December 24, 2021.

Contact information

Please contact us via our website.