24-R&D-0256

Vulnerabilities in PLC regarding plaintext transmission of sensitive information and predictable ID usage

IDEC Corporation

Published date: August 29, 2024

Overview

It has been discovered that our PLCs contain vulnerabilities related to the "Cleartext Transmission of Sensitive Information" (CWE-319) and the "Generation of Predictable Identifiers" (CWE-340).

CVSS

- Cleartext Transmission of Sensitive Information (CWE-319)
  - CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score: 4.6
  - CVE-2024-41927
- Generation of Predictable Identifiers (CWE-340)
  - CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score: 5.3
  - CVE-2024-28957

Affected products

The following products and software versions are affected.

Product name	Software version	CVE
FC6A Series MICROSmart All-in-One CPU module	Ver.2.60 and earlier	CVE-2024-41927 CVE-2024-28957
FC6B Series MICROSmart All-in-One CPU module	Ver.2.60 and earlier	
FC6A Series MICROSmart Plus CPU module	Ver.2.40 and earlier	
FC6B Series MICROSmart Plus CPU module	Ver.2.60 and earlier	
FT1A Series SmartAXIS Pro/Lite	Ver.2.41 and earlier	CVE-2024-41927

Description of vulnerabilities

- Cleartext Transmission of Sensitive Information (CVE-2024-41927)

  If an attacker sends specific commands via the PLC's serial communications port, they may be able to obtain user authentication information.
- Generation of Predictable Identifiers (CVE-2024-28957)

  Some of the IDs included in the headers of packets sent by the affected product may be predicted, resulting in the disruption of communications.

Impact

- ➢ Cleartext Transmission of Sensitive Information (CVE-2024-41927)

  By obtaining sensitive information such as user authentication information from communication data, it is possible that the PLC's program can be obtained, and the PLC may be operated illegally.

- ➢ Generation of Predictable Identifiers (CVE-2024-28957)

  There is a possibility that communications may be disrupted if an attacker uses predicted values for some of the IDs included in the headers of communication packets.

Countermeasures for Customers

The fixed products and software versions are as follows.

Product name	Software version
FC6A Series MICROSmart All-in-One CPU module	Ver.2.70 and later
FC6B Series MICROSmart All-in-One CPU module	Ver.2.70 and later
FC6A Series MICROSmart Plus CPU module	Ver.2.50 and later
FC6B Series MICROSmart Plus CPU module	Ver.2.70 and later
FT1A Series SmartAXIS Pro/Lite	Ver.2.50 and later

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

Mitigations/Workarounds

- ➢ Cleartext Transmission of Sensitive Information (CVE-2024-41927)

  Administer the PLC properly to prevent attackers from connecting to the PLC's serial communications port.

- ➢ Generation of Predictable Identifiers (CVE-2024-28957)

  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 August 29, 2024.

Contact information

Please contact us via our website.