24-R&D-0298

有关本公司 PLC 中重要信息的明文传输及可预测 ID 的使用方面的脆弱性事宜

IDEC 株式会社

公布日期 2024 年 8 月 29 日

■概述

本公司 PLC 在重要信息的明文传输(CWE-319)及可预测的 ID 使用(CWE-340)方面存在漏洞。

■CVSS 分数

- 重要信息的明文传输(CWE-319)
  - CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 基本分数： 4.6
  - CVE-2024-41927
- 可预测的 ID 使用(CWE-340)
  - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L 基本分数： 5.3
  - CVE-2024-28957

■该产品的确认方法

该产品及软件版本如下。

产品	软件版本	CVE
FC6A 型 MICROSmart All-in-One CPU 模块	Ver.2.60 及更早	CVE-2024-41927 CVE-2024-28957
FC6B 型 MICROSmart All-in-One CPU 模块	Ver.2.60 及更早	
FC6A 型 MICROSmart Plus CPU 模块	Ver.2.40 及更早	
FC6B 型 MICROSmart Plus CPU 模块	Ver.2.60 及更早	
FT1A 型控制器 SmartAXIS Pro/Lite	Ver.2.41 及更早	CVE-2024-41927

■脆弱性的说明

- 重要信息的明文传输 (CVE-2024-41927)

  攻击者可能会从 PLC 的串行通信端口发送特定命令从而获得用户的认证信息。
- 可预测 ID 的使用 (CVE-2024-28957)

  通过预测该产品发送的数据包标头中包含的部分 ID 从而干扰通信。

■脆弱性带来的威胁

- 重要信息的明文传输 (CVE-2024-41927)
  通过从通信数据中获取用户认证信息等重要信息，可能会获取 PLC 程序从而导致 PLC 被非法操作。
- 可预测 ID 的使用 (CVE-2024-28957)
  第三方使用通信包标头中包含的部分 ID 的预测值，则可能会受到通信干扰。

■对策方法

已修复漏洞的产品及软件版本如下。

产品	软件版本
FC6A 型 MICROSmart All-in-One CPU 模块	Ver.2.70 及更高
FC6B 型 MICROSmart All-in-One CPU 模块	Ver.2.70 及更高
FC6A 型 MICROSmart Plus CPU 模块	Ver.2.50 及更高
FC6B 型 MICROSmart Plus CPU 模块	Ver.2.70 及更高
FT1A 型控制器 SmartAXIS Pro/Lite	Ver.2.50 及更高

请从本公司的主页下载各软件的最新版本进行更新。

■缓解措施・回避措施

- 重要信息的明文传输(CVE-2024-41927)
  请妥善管理 PLC 以防止攻击者连接到 PLC 的串行通信端口。
- 可预测 ID 的使用(CVE-2024-28957)
  为了最大限度的降低利用此漏洞的风险，请使用专用网络或 VPN 等封闭网络。详情请参阅本公司主页上的“安全注意事项”。

■更新履历

2024 年 8 月 29 日　公布了此脆弱性信息页面。

■咨询方式

请通过本公司主页进行咨询。