有关本公司 PLC 脆弱性的事宜

IDEC 株式会社

公布日期 2021 年 12 月 24 日
最终更新日期 2021 年 12 月 24 日

■概述

因本公司 PLC 及其编程软件对认证信息的保护不足，而存在认证信息泄漏的漏洞。攻击者通过通信数据或编程软件创建的文件来获取认证信息，从而可能对 PLC 进行非法操作。（CVE-2021-37400、CVE-2021-37401、CVE-2021-20826、CVE-2021-20827）

■CVSS 分数

CVE-2021-37400 CVSS：3.1/AV：A/AC：L/PR：N/UI：N/S：U/C：H/I：L/A：L 基本分数：7.6
CVE-2021-37401 CVSS：3.1/AV：A/AC：L/PR：N/UI：N/S：U/C：H/I：L/A：L 基本分数：7.6
CVE-2021-20826 CVSS：3.1/AV：A/AC：L/PR：N/UI：N/S：U/C：H/I：L/A：L 基本分数：7.6
CVE-2021-20827 CVSS：3.1/AV：A/AC：L/PR：N/UI：N/S：U/C：H/I：L/A：L 基本分数：7.6

■该产品的确认方法

该产品及软件版本如下。

产品	软件版本
FC6A 型 MICROSmart All-in-One CPU 模块	2.32 及更早
FC6B 型 MICROSmart All-in-One CPU 模块	2.31 及更早
FC6A 型 MICROSmart Plus CPU 模块	1.91 及更早
FC6B 型 MICROSmart Plus CPU 模块	2.31 及更早
FT1A 型控制器 SmartAXIS Pro/Lite	2.31 及更早
WindLDR	8.19.1 及更早
数据文件管理器	2.12.1 及更早
WindEDIT Lite	1.3.1 及更早

■脆弱性的说明

因本公司 PLC 及其编程软件对认证信息的保护不足，而存在通过通信数据或编程软件创建的文件获取认证信息的漏洞。

■脆弱性带来的威胁

恶意攻击者可能会利用认证信息，对 PLC 内的程序进行读取、改写等非法操作。

■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	2.40 及更高
FC6B 型 MICROSmart All-in-One CPU 模块	2.40 及更高
FC6A 型 MICROSmart Plus CPU 模块	2.00 及更高
FC6B 型 MICROSmart Plus CPU 模块	2.40 及更高
FT1A 型控制器 SmartAXIS Pro/Lite	2.40 及更高
WindLDR	8.20.0 及更高
数据文件管理器	2.13.0 及更高
WindEDIT Lite	1.4.0 及更高

请从本公司主页下载上传各个软件的最新版本。

■缓解措施・回避措施

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

2021 年 12 月 24 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。