机械自动化控制器 NJ/NX 存在数据真实性验证不足的漏洞

发布日期：2024 年 5 月 27 日

欧姆龙株式会社

■概要

欧姆龙一直致力于在工业自动化领域为客户提供安全、可靠、高质量的产品与解决方案，这是我们立足行业，持续助推客户业务增长，为客户创造价值的根基。

近期，我们发现机械自动化控制器 NJ/NX 系列存在数据真实性验证不足（CWE-345）的漏洞。攻击者可利用本漏洞使控制器产品无法检测到产品内的用户程序已被篡改。

为了使您的安全得到有效保护，我们第一时间采取行动，排查受该漏洞影响的产品和版本，并推出相应对策、以及减轻措施/解决方法。您可以通过下述推荐的减轻措施/解决方法，实现将该漏洞的恶意利用风险降至最低。

■对象产品

受此漏洞影响的产品型号及版本如下所示。

- 机械自动化控制器 NJ 系列 CPU 单元 所有版本
- 机械自动化控制器 NX 系列 CPU 单元 所有版本

■漏洞内容

机械自动化控制器 NJ/NX 系列存在数据真实性验证不足（CWE-345）的漏洞，攻击者可利用本漏洞使控制器产品无法检测到产品内的用户程序已被篡改。

■CVSS 评分

数据真实性验证不足（CWE-345）

CVE-2024-33687

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N 基础评分 4.8

■对策方法

将各产品更新至对策版本以应对漏洞。

1. 使用没有用户程序恢复信息的传输功能

   通常，将用户程序从 Sysmac Studio 传输到 CPU 单元时，用于恢复程序的信息也会被传输。此时，由于本功能不传输用于恢复程序的信息，因此用户程序无法被篡改。确认使用方法，请参见以下手册的“没有用户程序恢复信息的传输功能”。

   - NJ/NX 系列 CPU 单元 用户手册 软件篇（SBCA-CN5-467）

■减轻措施/解决方法

为了实现将这些漏洞的恶意利用风险降至最低，我们十分建议您采取以下减轻措施。

1. 防病毒保护

   在连接控制系统的电脑上安装最新版本的企业级杀毒软件，并定期维护。

2. 防止未经授权的访问

   推荐采取以下措施。

   - 最大限度地减少控制系统或设备的网络连接，禁止不受信任的设备访问
   - 通过部署防火墙隔离 IT 网络（断开未使用的通信端口、限制通信主机）
   - 需要远程访问控制系统或设备时，使用虚拟专用网络（VPN）
   - 使用高强度密码并定期修改
   - 引入物理控制，确保仅授权人员可访问控制系统和设备
   - 在控制系统或设备中使用 USB 存储器等外部存储设备时，事先进行病毒扫描
   - 在远程访问控制系统或设备时进行多重要素验证

3. 数据输入/输出保护

   确认备份和范围检查等设置的合理性，以防对控制系统和设备的输入/输出数据的意外修改

4. 恢复丢失的数据

   定期对设置数据进行备份和维护，以防数据丢失

■咨询方式

如您在采取减轻措施/解决方法时遇到问题，可以通过下列方式向我们的事务所或经销商咨询：

https://www.fa.omron.com.cn/contactus

■谢辞

Microsoft 公司 CPS Research Team 的 Tamir Ariel 先生报告了本漏洞。

我们在此感谢发现并报告了漏洞的 Tamir Ariel 先生。

■更新记录

2024 年 5 月 27 日创建