机械自动化控制器 NJ/NX 系列
中的恶意程序执行漏洞

发布日期：2022 年 12 月 21 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，我们发现在机械自动化控制器 NJ/NX 系列中，存在数字签名输入验证不当（CWE-347）的漏洞。攻击者可能会利用该漏洞执行恶意程序。

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。

此外，为了确保您安心使用本产品，我们还为受该漏洞影响的产品准备了安全增强的对策版本。您可在下文“对策方法”处查找对应的对策版本。

■对象产品

受本漏洞影响的产品型号及版本如下：

系列	型号	适用版本
机械自动化控制器 NX7 系列	所有型号	V1.28 及以下
机械自动化控制器 NX1 系列	所有型号	V1.48 及以下
机械自动化控制器 NJ 系列	所有型号	V1.48 及以下

对象产品版本的确认方法请参阅以下手册中的“Checking Versions”部分：

- NX 系列 CPU Unit User's Manual (Hardware)（W535-E1）
- NX 系列 NX102 CPU Unit User's Manual (Hardware)（W593-E1）
- NX 系列 NX1P2 CPU Unit User's Manual (Hardware)（W578-E1）
- NJ 系列 CPU Unit User's Manual (Hardware)（W500-E1）

■漏洞内容

在机械自动化控制器 NJ/NX 系列中，由于存在数字签名输入验证不当（CWE-347）的漏洞，可能对该产品非法执行任意对象代码。

■漏洞可能造成的威胁

攻击者可能会利用该漏洞，将针对该产品的恶意程序传输到控制器并非法执行。

■CVSS 评分

数字签名输入验证不当（CWE-347）

CVE-2022-31206

CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:N　　基础评分: 4.4

■减轻措施/解决方法

为了实现将该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.防止非法访问

- 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。
- 通过部署防火墙来隔离 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。

■对策方法

您还可以将受漏洞影响的产品更新为对策版本，以增强其安全性。

以下是各产品的对策版本：

系列	型号	对策版本
机械自动化控制器 NX7 系列	所有型号	V1.29 及以上版本
机械自动化控制器 NX1 系列	所有型号	V1.50 及以上版本

机械自动化控制器 NJ 系列	NJ501-1300 NJ501-1400 NJ501-1500	V1.49 及以上版本
	上述以外的其他型号	V1.50 及以上版本

上述对策版本固件的获取途径及更新方法，可咨询我们的营业部门了解。

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

您还可以通过使用控制器的安全功能，有效防止第三方非法传输程序。功能详情、设置方法请参阅。NJ/NX 系列 CPU 单元用户手册 软件篇（Cat.No.501）[8-5 安全功能]。

- 使用用户认证功能，在工具在线时对每个用户进行认证，实现仅能根据用户的权限进行操作，以此防止非法访问。
- 使用 Packet Filter 功能，通过内置 EtherNet/IP 端口的接收处理来过滤 IP 数据包，以此对外部的非法访问施加限制。
- 使用安全通信功能，通过对 Sysmac Studio 或 NA 系列与控制器的通信数据进行加密，以此防止第三方窃听或篡改数据。

■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

■其他

该漏洞及其应对措施建议来源于欧姆龙相关外部机构对外公开的内容：

・JVN: JVNVU#97111518
欧姆龙的 SYSMAC CS/CJ/CP 系列和 NJ/NX 系列中的多个漏洞
https://jvn.jp/vu/JVNVU97111518/

・CISA：ICS Advisory (ICSA-22-179-02)
Omron SYSMAC CS/CJ/CP Series and NJ/NX Series
https://www.cisa.gov/uscert/ics/advisories/icsa-22-179-02

■更新记录

2022/12/21　创建