

机械自动化控制器 NJ/NX 系列存在路径遍历漏洞

发布日期：2024 年 3 月 7 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 系列存在路径遍历（CWE-22）漏洞。攻击者可利用本漏洞获得对控制器产品未经授权的访问、远程执行代码。

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。

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

受此漏洞影响的产品型号及版本如下所示。

系列	型号	适用版本
机械自动化控制器 NJ 系列	NJ101-□□□□	Ver.1.64.03 以下
	NJ301-□□□□	Ver.1.64.00 以下
	NJ501-1□0□	Ver.1.64.03 以下
	NJ501-1□2□	Ver.1.64.00 以下
	NJ501-1340	Ver.1.64.00 以下
	NJ501-4□□□	Ver.1.64.00 以下
	NJ501-5300	Ver.1.64.00 以下
	NJ501-R□□□	Ver.1.64.00 以下
机械自动化控制器 NX 系列	NX1P2-□□□□□□	Ver.1.64.00 以下
	NX1P2-□□□□□□1	Ver.1.64.00 以下
	NX102-□□□□	Ver.1.64.00 以下
	NX502-□□□□	Ver.1.65.01 以下
	NX701-□□□□	Ver.1.35.00 以下
	NX-EIP201	Ver.1.00.01 以下

确认对象产品版本的方法，请参见“附件-产品版本的确认方法”。

■漏洞内容

机械自动化控制器 NJ/NX 系列存在路径遍历（CWE-22）漏洞，攻击者可利用本漏洞获得对控制器产品未经授权的访问、远程执行代码。

■CVSS 评分

路径遍历（CWE-22）

CVE-2024-27121

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H 基础评分 7.2

■对策方法

将各产品更新至对策版本以应对漏洞。

各产品的对策版本与发布日期见下表。

系列	型号	计划对策版本	对策版本 计划推出时间
机械自动化控制器 NJ 系列	NJ101-□□□□	Ver.1.64.04 以上	2024 年 4 月
	NJ301-□□□□	Ver.1.64.04 以上	2024 年 4 月
	NJ501-1□0□	Ver.1.64.04 以上	2024 年 4 月
	NJ501-1□2□	Ver.1.64.04 以上	2024 年 4 月
	NJ501-1340	Ver.1.64.04 以上	2024 年 4 月
	NJ501-4□□□	Ver.1.64.04 以上	2024 年 4 月
	NJ501-5300	Ver.1.64.04 以上	2024 年 4 月
	NJ501-R□□□	Ver.1.64.04 以上	2024 年 4 月
机械自动化控制器 NX 系列	NX1P2-□□□□□□	Ver.1.64.04 以上	2024 年 4 月
	NX1P2-□□□□□□1	Ver.1.64.04 以上	2024 年 4 月
	NX102-□□□□	Ver.1.64.04 以上	2024 年 4 月
	NX502-□□□□	Ver.1.66.00 以上	2024 年 4 月
	NX701-□□□□	Ver.1.35.04 以上	2024 年 4 月
	NX-EIP201	Ver.1.01.00 以上	2024 年 4 月

上述对策版本的获取途径及更新方法，请咨询本公司销售窗口。

■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. 使用安全通信功能

安全通信功能可防止数据被第三方窃听或篡改。安全通信功能可用于以下 CPU 单元的单元版本。

- NJ 系列、NX102、NX1P2 CPU 单元：Ver.1.49 以上

- NX701 CPU 单元：Ver.1.29 以上
- NX502 CPU 单元：Ver.1.60 以上
- NX-EIP201：Ver.1.00 以上

2. 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。

3. 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

4. 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

5. 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。

Dragos 公司 Principle Vulnerability Analyst 的 Logan Carpenter 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 先生和 Logan Carpenter 先生。

■ 更新记录

2024 年 3 月 7 日创建

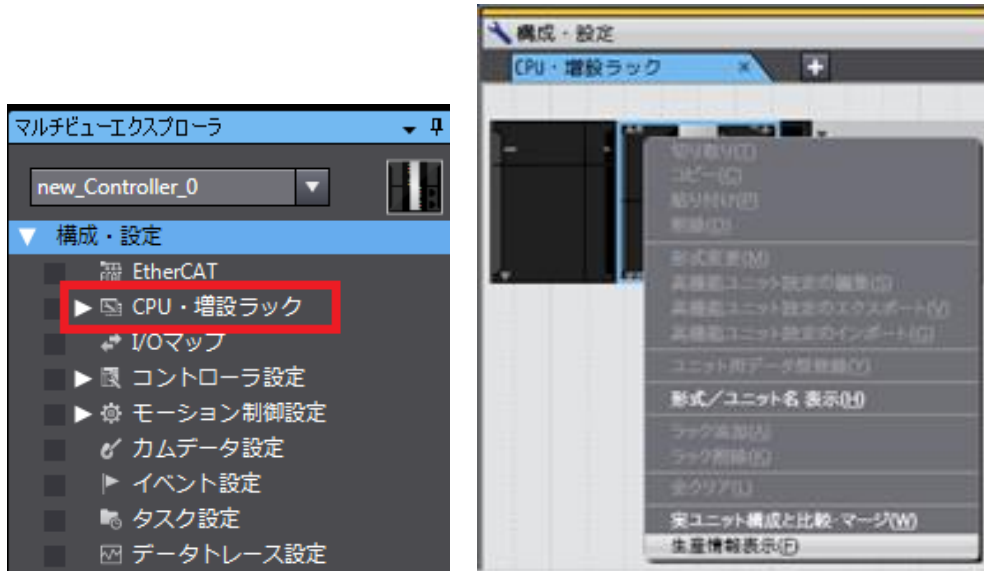
附件-产品版本的确认方法

确认产品版本的方法因产品系列而异。

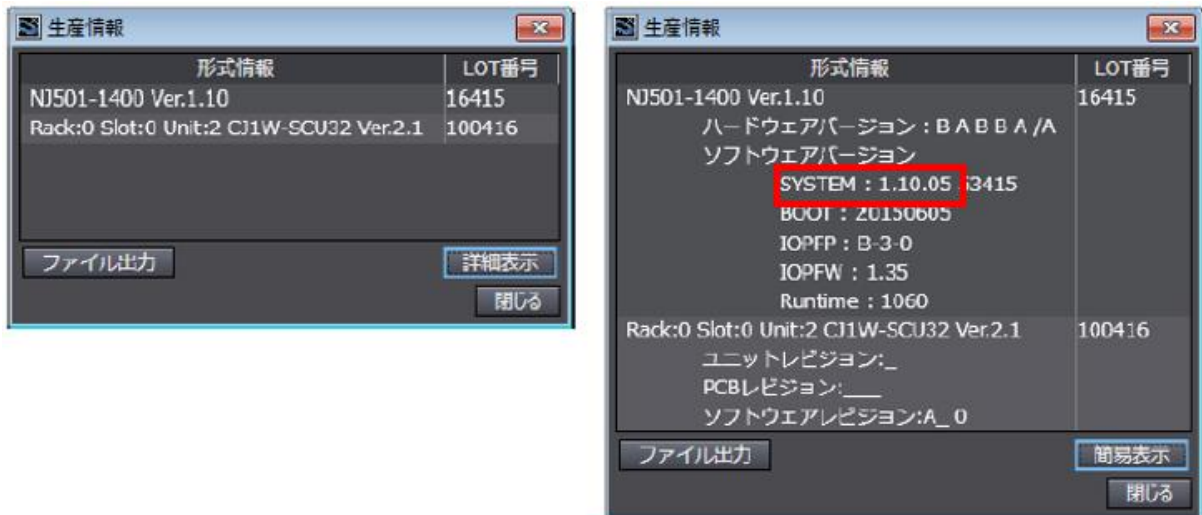
NJ 系列的确认方法

在 Sysmac Studio 的 Multi View Explorer 中双击[配置/设置] → [CPU/扩展机架]。

右键单击单元编辑器中的空白字段，然后选择[显示生产信息]。



选择[生产信息]→[详细显示]。下图显示了 Ver.1.10.05。



NX 系列的确认方法

在 Sysmac Studio 的 Multi View Explorer 中右键单击[配置/设置]的[CPU/扩展机架]的[CPU 机架]，然后选择[显示生产信息]。将显示[生产信息]对话框。



在[生产信息]对话框的右下角选择[简单显示]或[详细显示]。切换[生产信息]的简单显示和详细显示。下图显示了 NX502-1500 的 Ver.1.60.02 和 NX-EIP201 的 Ver.1.00.00。

