NJ/NX 系列机械自动化控制器中的恶意程序执行漏洞

发布日期：2022 年 7 月 1 日
更新日期：2022 年 10 月 11 日
欧姆龙株式会社

■概述

在 NJ/NX 系列机械自动化控制器中发现，利用遗留的调试代码(CWE-489)，执行恶意程序的可能性。攻击者非法访问该产品之后，利用此漏洞执行恶意程序，使该产品拒绝服务。

受该漏洞影响的产品、版本及缓解措施和规避方法见下文。通过实施这些推荐的缓解措施和规避方法可以将这些漏洞的恶意利用风险降至最低。此外，为确保客户安心使用我们的产品，我们还为每个产品提供了安全增强对策版本。相关对策见下文，请根据需要实施相应的对策。

■受影响产品

受影响的产品及其版本如下所示。

产品系列	型号	版本
NX7 系列机械自动化控制器	所有型号	1.28 或更低
NX1 系列机械自动化控制器	所有型号	1.48 或更低
NJ 系列机械自动化控制器	所有型号	1.48 或更低

请参阅下列手册，了解如何查看目标产品的版本。

- NX 系列 CPU 单元硬件用户手册 (W535)
- NX 系列 NX102 CPU 单元硬件用户手册 (W593)
- NX 系列 NX1P2 CPU 单元硬件用户手册 (W578)
- NJ 系列 CPU 单元硬件用户手册 (W500)

请参阅上述手册中的“查看版本”部分。

■说明

在 NJ/NX 系列机械自动化控制器中发现，利用遗留的调试代码(CWE-489)，执行恶意程序的可能性。攻击者非法访问该产品之后，利用此漏洞执行恶意程序，使该产品拒绝服务。

■潜在威胁和影响

攻击者可能利用漏洞引发产品故障或执行恶意程序。

■CVSS 评分

CVE-2022-33971

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H 基础评分 8.3

■缓解措施和规避方法

为了将这些漏洞的恶意利用风险降至最低，欧姆龙建议客户采取下列缓解措施。

1.防病毒保护

保护所有可访问控制系统的个人电脑，防止其被恶意软件攻击，确保安装并维护最新版本的企业级杀毒软件。

2.采取安全措施，防止未授权访问

- 最大限度地减少控制系统和设备与开放网络的连接，以防不受信任设备访问控制系统和设备。
- 使用防火墙（关闭未使用的通信端口，限制通信主机），将其与 IT 网络隔离。
- 使用虚拟专用网络 (VPN) 远程访问控制系统和设备。
- 使用强密码并经常修改。
- 安装物理控制设施，确保仅授权人员可访问控制系统和设备。
- 连接系统和设备之前，扫描病毒，确保 USB 设备或类似设备安全。
- 尽可能对远程访问控制系统和设备的所有设备均执行多重要素验证。

3.数据输入和输出保护

采用备份和范围检查等验证处理措施，以防控制系统和设备输入/输出数据被无意修改。

4.数据恢复

定期进行数据备份和维护，以防数据丢失。

■对策

可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。

产品系列	型号	版本	发布日期
NX7 系列机械自动化控制器	所有型号	1.29 或更高	2022 年 10 月 11 日
NX1 系列机械自动化控制器	所有型号	1.50 或更高	2022 年 10 月 11 日
NJ 系列机械自动化控制器	NJ501-1300 NJ501-1400 NJ501-1500	1.49 或更高	2022 年 7 月 1 日
	除上述型号以外	1.50 或更高	2022 年 10 月 11 日

有关如何获取和更新产品对策版本固件的信息，请联系我们的销售办事处或经销商。您可以用安装的 Omron Automation Software Auto Update（欧姆龙自动化软件自动更新）工具，将 Sysmac Studio 更新至最新版本。

■联系信息

请联系我们的事务所或经销商。

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

■其他

本文档中的漏洞和对策与美国网络安全和基础设施安全局 (CISA) 在下方报告的漏洞攻击工具所使用的漏洞和对策相符。

适用于 ICS/SCADA 设备的 APT 网络工具

https://www.cisa.gov/uscert/ncas/alerts/aa22-103a

■更新历史

- 2022 年 7 月 1 日：新版本
- 2022 年 10 月 11 日：更新以下 2 项内容

（1）更新【对策】中对策版本的发布日期

（2）变更本漏洞（CVE-2022-33971）的 CWE 编号及 CVSS 评分

（变更前）捕获-回放绕过身份验证(CWE-294)

CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H 基础评分 7.6

（变更后）残留调试编码（CWE-489）

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H 基础评分 8.3