NJ/NX 系列机械自动化控制器通信功能中的认证绕过漏洞

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

NJ/NX 系列机械自动化控制器、自动化软件 Sysmac Studio 和 NA 系列可编程终端之间的通信功能存在使用硬编码凭证 (CWE-798) 和通过捕获-回放绕过身份验证 (CWE-294) 的漏洞。攻击者可能利用这些漏洞绕过通信连接过程中的身份验证，然后非法访问控制器产品。

受这些漏洞影响的产品、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 系列接卸自动化控制器	所有型号	1.48 或更低
自动化软件 Sysmac Studio	所有型号	1.49 或更低
NA 系列 可编程终端	NA5-15W NA5-12W NA5-9W NA5-7W	运行时版本 1.15 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。

- NA 系列可编程终端硬件用户手册 (V117)
- NA 系列可编程终端硬件 (-V1) 用户手册 (V125)

请参阅上述手册中的“系统菜单概述”部分。（运行时版本位于系统菜单界面的左下方区域。）

・ Sysmac Studio 第 1 版操作手册 (W504)

请参阅上述手册中的“显示和注册许可证”部分。

■说明

由于 NJ/NX 系列机械自动化控制器、自动化软件 Sysmac Studio 和 NA 系列可编程终端之间的通信功能存在使用硬编码凭证 (CWE-798) 和通过捕获-回放绕过身份验证 (CWE-294) 的漏洞，产品可能被非法登录并操作。

■潜在威胁和影响

攻击者可能利用这些漏洞绕过通信连接过程中的身份验证，然后非法登录并操作控制器产品。

■CVSS 评分

1) 使用硬编码凭证 (CWE-798)

CVE-2022-34151

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H 基础评分 9.4

2) 通过捕获-回放绕过身份验证 (CWE-294)

CVE-2022-33208

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H 基础评分 7.5

■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
自动化软件 Sysmac Studio	所有型号	1.50 或更高	2022 年 7 月 1 日
NA 系列 可编程终端	NA5-15W NA5-12W NA5-9W NA5-7W	运行时版本 1.16 或更高	2022 年 7 月 1 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 AutoUpdate（欧姆龙自动化软件自动更新）工具，将 Sysmac Studio 更新至最新版本。

另外，我们还建议使用控制器的以下安全功能，采取安全措施。具体功能、设定方法等请参阅 NJ/NX 系列 CPU 单元用户手册 软件篇（Cat.No.501）[8-5 安全功能]。

-使用安全通信功能，将 Sysmac Studio、NA 系列可编程终端与控制器间的通信数据进行加密。可以防止数据的盗取或篡改。

-使用 Packet Filter 功能，在内置 EtherNet/IP 端口进行 IP 包过滤。可以限制来自外部的非法访问。

-使用用户认证功能，对在线用户逐一认证和设置用户权限之后，进行在线连接操作。可以限制来自外部的非法访问。

■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

本文档中的这些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）变更如下漏洞评分信息

・CVE-2022-34151 CVSS 评分

（变更前）CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H 基础评分 7.7

（变更后）CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H 基础评分 9.4

・CVE-2022-33208 CVSS 评分

（变更前）CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:H/A:H 基础评分 6.2

（变更后）CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H 基础评分 7.5