自动化软件 Sysmac Studio

及 NX-IO Configurator 存在路径遍历漏洞

发布日期：2023 年 9 月 19 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，我们发现自动化软件 Sysmac Studio 及 NX-IO Configurator 存在路径遍历（CWE-22）漏洞。攻击者可利用本漏洞将文件放置于电脑中的任意路径。

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

受本漏洞影响的产品型号及版本如下所示。

产品名称	型号	适用版本
自动化软件 Sysmac Studio	SYSMAC-SE2□□□	Ver.1.54 以下
NX-IO Configurator	CX-One CXONE-AL□□D-V4 附带	Ver.1.22 以下

确认对象产品版本的方法请参见以下手册。

- SYSMAC-SE2□□□ Sysmac Studio Version 1 Operation Manual（W504）
- NX-IO Configurator Operation Manual（W585）

■漏洞内容

自动化软件 Sysmac Studio 及 NX-IO Configurator 存在路径遍历（CWE-22）漏洞，攻击者可利用本漏洞将文件放置于任意位置。

■漏洞可能造成的威胁

攻击者可利用本漏洞将恶意文件放置于目标电脑中，进而不经授权操作电脑。

■CVSS 评分

路径遍历（CWE-22）

CVE-2018-1002205

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N 基础评分 5.5

■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

- 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

■对策方法

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。

产品名称	型号	对策版本	发布日期
自动化软件 Sysmac Studio	SYSMAC-SE2□□□	V1.55 以上	2023 年 7 月 18 日
NX-IO Configurator	CX-One CXONE-AL□□D-V4 附带	V1.23 以上	2023 年 4 月 24 日

上述对策版本的获取途径及更新方法，请通过下述咨询方式咨询本公司。

■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

Dragos 公司的 Reid Wightman 先生通过 CISA 报告了本漏洞。

Michael Heinzl 先生通过 JPCERT/CC 报告了本漏洞。

我们在此感谢发现并报告了漏洞的 Reid Wightman 先生和 Michael Heinzl 先生。

■更新记录

2023 年 9 月 19 日创建