Sysmac Studio/CX-One 通用模块中存在释放不在缓存开始位置的指针漏洞

发布日期：2024 年 4 月 22 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 Sysmac Studio/CX-One 通用模块中存在释放不在缓存开始位置的指针（CWE-761）漏洞。攻击者可利用这些漏洞执行任意代码。

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

受本漏洞影响的产品型号及版本如下所示。

系列	型号	适用版本
CX-One	CX-One CXONE-AL□□D-V4	通过 DVD 安装至 CX-One Ver.4.61.1 版本，以及在此基础上 CX-One 自动更新（适用于 V4_2024 年 1 月）的任意更新版本
Sysmac Studio	SYSMAC-SE2□□□	通过 DVD 安装至 Sysmac Studio Ver.1.56 版本，以及在此基础上截至 2024 年 1 月 Sysmac Studio V1 自动更新的任意更新版本

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

Sysmac Studio/CX-One 通用模块中存在释放不在缓存开始位置的指针（CWE-761）漏洞，攻击者可利用这些漏洞执行任意代码。

■CVSS 评分

释放不在缓存开始位置的指针（CWE-761）

CVE-2024-31413

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H 基础评分 7.8

■对策方法

可以通过更新 Sysmac Studio/CX-One 通用模块的通用组件以应对漏洞。

各产品的对策版本与发布日期见下表。

系列	型号	对策版本	对策版本 推出时间
CX-One	CX-One CXONE-AL□□D-V4	应用 CX-One 自动更新（适用于V4_2024年04 月）以上版本	2024 年 4 月 22 日
Sysmac Studio	SYSMAC-SE2□□□	应用 2024 年 04 月 Sysmac Studio V1 自动更新以上版本（Ver.1.58 以上）	2024 年 4 月 22 日

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. 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

   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

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

■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

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 Michael Heinzl 先生。

■更新记录

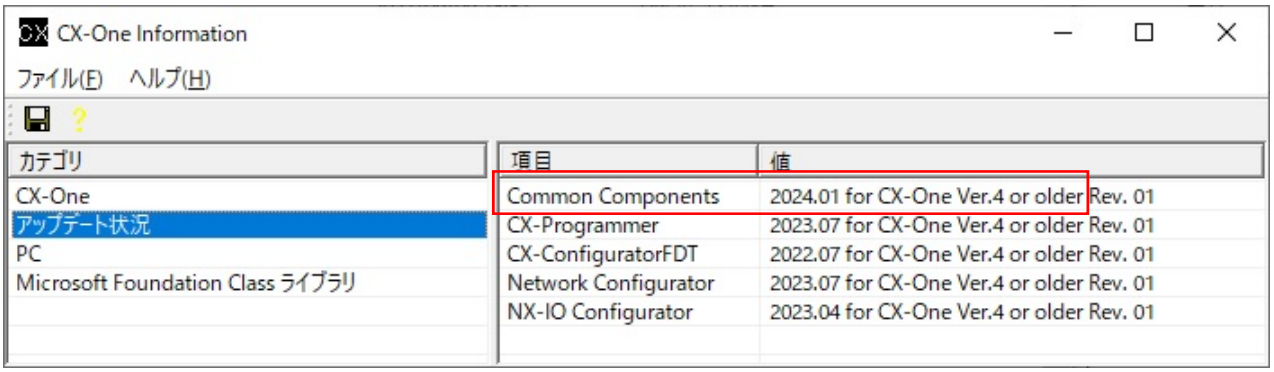
2024 年 4 月 22 日创建

附件-产品版本的确认方法

CX-One 的确认方法

从开始菜单 - [Omron] - [CX-One] - [CX-One Information]启动 CX-One Information，然后从[Update Status]确认 Common Components 的值。

※以下示例为已安装 CX-One 自动更新（适用于 V4_2024 年 01 月）的显示。



Sysmac Studio 的确认方法

在 Sysmac Studio 首页点击[License]，确认模块版本的值。