变频器/伺服用支持软件 CX-Drive 中的

基于堆的缓冲区溢出漏洞

发布日期：2023 年 4 月 24 日

更新日期：2023 年 8 月 1 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，我们发现在变频器/伺服用支持软件 CX-Drive 中存在基于堆的缓冲区溢出漏洞（CWE-122)。本地攻击者可恶意利用该漏洞引发信息泄露，或在受影响的 CX-Drive 的安装上执行任意代码。 恶意利用该漏洞需要用户的操作，用户打开恶意 SDD 文件是攻击者进行攻击的必要条件。

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。

■对象产品

受本漏洞影响的产品型号及版本如下。

系列	型号	适用版本
CX-Drive	全型号	所有版本

对象产品版本的确认方法请参见以下手册。

・CX-Drive Operation User's Manual（W453-E1）

■CVSS 评分

基于堆的缓冲区溢出漏洞（CWE-122）

CVE-2023-27385

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

■减轻措施/解决方法

为将该漏洞的恶意利用风险降至最低，建议采取以下减轻措施。

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。

・不执行可疑程序文件

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

・通过部署防火墙来隔离 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

5. 采用新型软件工具和控制器

・自动化软件 Sysmac Studio

・控制器 NJ/NX/NY 系列

■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

2023/04/24 创建

2023/8/1 更新适用版本