# CX-Programmer 的越界读取、基于堆的缓冲区溢出、以及使用已释放内存的漏洞

发布日期：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 CX-Programmer 存在越界读取（CWE-125）导致内存损坏、基于堆的缓冲区溢出（CWE-122）、以及使用已释放内存（CWE-416）的漏洞。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

受这些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 |
|---|---|---|
| CX-Programmer | CX-One CXONE-AL□□D-V4 附带 | V9.80 以下 |

确认对象产品版本的方法请参见以下手册。

- CX-Programmer Ver.9.□ 操作手册（W446）

■漏洞内容

CX-Programmer 存在越界读取（CWE-125）导致内存损坏、基于堆的缓冲区溢出（CWE-122）及使用已释放内存（CWE-416）的漏洞。

■漏洞可能造成的威胁

攻击者可利用这些漏洞执行任意代码。

■CVSS 评分

越界读取（CWE-125）

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

基于堆的缓冲区溢出（CWE-122）
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

使用已释放内存（CWE-416）
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 |
|---|---|---|---|
| CX-Programmer | CX-One CXONE-AL□□D-V4 附带 | V9.81 以上 | 2023 年 7 月 3 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。

■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

2023 年 8 月 1 日创建