可编程控制器 CP 系列 Ethernet 选项板

中 Web 浏览器功能的密码泄露漏洞

发布日期：2022 年 12 月 21 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，我们发现在可编程控制器 CP 系列中，存在凭证信息明文存储（CWE-256）的漏洞。攻击者可能会利用该漏洞非法访问该控制器产品。

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

受该漏洞影响的产品型号及版本如下：

系列	型号	对象版本
SYSMAC CP 系列	CP1W-CIF41	所有版本

对象产品版本的确认方法请参阅以下手册：

・CP1H CPU Unit Operation Manual（W450-E1）

「Unit Versions of CP-series CPU Units」、「9-10 Web Browser Setup and Display」

・CP1L CPU Unit Operation Manual（W462-E1）

「Unit Versions of CP-series CPU Units」、「9-10 Web Browser Setup and Display」

・CP1E CPU Unit User's Manual (Hardware)（W479-E1）
「2-2-3 Unit Versions of CPU Units」
・CP1E CPU Unit User's Manual (Software)（W480-E1）
「17-3 Settings」

■漏洞内容

在可编程控制器 CP 系列中，由于凭证信息明文存储（CWE-256）的漏洞，存在可以非法访问该控制器产品的漏洞。

■漏洞可能造成的威胁

攻击者可能会利用该漏洞，非法窃取 Ethernet 选项板（CP1W-CIF41）的 Web 浏览器功能的密码，从而导致控制器的设置变更或信息泄露。

■CVSS 评分

凭证信息明文存储（CWE-256）

CVE-2022-31205

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N 基础评分 6.5

■减轻措施/解决方法

为了实现将该漏洞的恶意利用风险降至最低，您可以将 Ethernet 选项板（CP1W-CIF41）的 Web 浏览器功能密码设置为与 CP1 主机密码不同的密码，从而降低密码泄露风险。

有关设置方法，请参阅以下手册：

・CP1H CPU Unit Operation Manual（W450-E1）
「Unit Versions of CP-series CPU Units」、「9-10 Web Browser Setup and Display」
・CP1L CPU Unit Operation Manual（W462-E1）
「Unit Versions of CP-series CPU Units」、「9-10 Web Browser Setup and Display」
・CP1E CPU Unit User's Manual (Software)（W480-E1）
「17-3 Settings」

此外，我们十分建议您同时采取以下对应措施：

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.防止非法访问

- 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，以防止数据丢失。

■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

■其他

该漏洞及其应对措施建议来源于欧姆龙相关外部机构对外公开的内容：

・JVN: JVNVU#97111518

欧姆龙的 SYSMAC CS/CJ/CP 系列和 NJ/NX 系列中的多个漏洞

https://jvn.jp/vu/JVNVU97111518/

・CISA：ICS Advisory (ICSA-22-179-02)

Omron SYSMAC CS/CJ/CP Series and NJ/NX Series

https://www.cisa.gov/uscert/ics/advisories/icsa-22-179-02

■更新记录

2022/12/21 创建