关于多款欧姆龙产品安装的FINS协议中存在的已知问题

发布日期：2023年04月17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。

FINS（Factory Interface Network Service，工厂接口网络服务），是用于由欧姆龙公司产品构成的FA网络中的信息通信协议。此次将欧姆龙公司的可编程控制器（PLC）中存在由FINS协议引发的已知问题、以及相应对策方法进行汇总联络。

■受影响的代表性设备

- SYSMAC CS系列 CPU单元 所有版本
- SYSMAC CJ系列 CPU单元 所有版本
- SYSMAC CP系列 CPU单元 所有版本
- SYSMAC NJ系列 CPU单元 所有版本
- SYSMAC NX1P系列 CPU单元 所有版本
- SYSMAC NX102系列 CPU单元 所有版本
- SYSMAC NX7数据库连接CPU单元（Ver.1.16以上）

■详细信息

FINS协议是一种轻量、简单的通信协议，用于控制欧姆龙公司生产的PLC和PC软件等FA（Factory Automation，工厂自动化）网络。FINS协议能够进行指令和响应式信息通信，从而监视、操作或设定FA控制系统。

FINS指令种类繁多，大致可分为以下几类。

・读取/写入I/O存储器区域

・读取/写入参数区域

・读取/写入程序区域

・变更动作模式

・读取设备结构

・读取CPU单元的状态

・访问时间信息

・读取/解除信息通信

・获取或释放访问权

・异常记录的读取等

・文件操作

・强制设置/复位

以上相关信息已在产品手册等资料中公开，规格式样也已经披露。不同型号所支持的FINS指令有所不同。

FINS指令信息由“FINS开头”、“FINS指令代码”和“参数”三部分构成。接受FINS指令信息的控制设备/软件会执行与该“FINS指令代码”对应的处理，并将处理结果作为FINS响应信息返回至包含在“FINS开头”中的发送目标。

当初设计FINS协议时，是基于FA网络是以工厂、生产线和设备内部的封闭化本地网络为前提。因此，在FA网络已成为开放网络的现在，对于FINS协议规格，被指出存在一些漏洞。

1.明文通信

FINS协议规格未对加密通信。因此，通信线路中的FINS消息以明文形式收发，易遭监听。此外，也无法检测FINS信息是否被篡改。

・机密信息的明文通信（CWE-319）

・未充分验证数据可靠性（CWE-345）

2.无需认证

FINS协议规格未对认证处理进行规定。因此无法识别是否遭受恶意通信对象攻击。

・通过欺骗回避认证（CWE-290）

・通过捕捉-回放攻击回避认证（CWE-294）

・缺失对关键功能的认证（CWE-306）

・未充分验证数据可靠性（CWE-345）

・干扰服务运行（DoS）的漏洞（CWE-400）

・对来自外部的操作的限制不完备（CWE-412）

・交互频率控制不当（CWE-799）

这些漏洞由 FINS 协议规格引发，但目前尚无修订规格的计划。

■预期影响

第三方可能会监听通信内容，执行非法控制指令或未经授权而访问控制系统信息。

■对策方法

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.不使用FINS（禁用FINS）

不在FA网络中使用FINS，即可防范由FINS协议规格引发的漏洞。例如，对于以下机型，可禁用FINS。

● SYSMAC NJ系列 CPU单元（Ver.1.49以上）

● SYSMAC NX1P系列 CPU单元（Ver.1.49以上）

● SYSMAC NX102系列 CPU单元（Ver.1.49以上）

● SYSMAC NX7数据库连接CPU单元（Ver.1.29以上）

2.防止未经授权的访问

可通过采取下述规避措施减轻漏洞的影响。

-限制访问来源的IP地址

-限制未经许可的网络访问

-启用FINS写入保护功能

-通过使用PLC保护密码限制写入权限

-通过使用PLC上的硬件指拨开关禁止变更PLC程序。

此外，还建议采取下列对策。

・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、限制对 FINS 端口(9600)的访问)。

・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.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。

4.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。

5. 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。

另外，已知问题详见如下说明及链接，请参照以及商讨对策。

・ICS Advisory (ICSA-20-063-03), Omron PLC CJ Series

https://www.us-cert.gov/ics/advisories/icsa-20-063-03

・ICS Advisory (ICSA-19-346-02), Omron PLC CJ and CS Series

https://www.us-cert.gov/ics/advisories/icsa-19-346-02

・ICS Advisory (ICSA-22-179-02), Omron SYSMAC CS/CJ/CP Series and NJ/NX Series

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

被报告存在已知问题的机型以外，如存在本文所述的FINS协议规格引发的漏洞，也作为已知问题进行处理。

■相关文件

-关于外部机构指出的本公司PLC的漏洞信息

https://www.omron-cxone.com/security/2019-12-06_PLC_EN.pdf

- CS/CJ/CP/NSJ系列样本 Communications Commands Reference Manual

（Cat. No. W342）

-NX系列样本 CPU Unit FINS Function User's Manual （（Cat. No. W596）

■更新记录

2023/04/17 创建