在发生涉及SOLAR-OT部署的CHIYU传感器事件后采取的补救行动

部署最新固件版本并加强SOLAR-OT监控平台

作者	验证人
Deirdre STARSKY，技术项目经理	Elena PIZARI，工业部总经理

目标

本文件说明了SOLAR-OT部署的访问控制系统发生事故后的2项补救措施：

1. 紧急部署所有系统的固件更新
2. 加强监督平台的配置

1. 紧急部署固件更新

制造商CHIYU已经为“SEMAC”访问控制系统开发了一个固件升级程序，可以修正该漏洞 => SOLAR-OT应在所有站点紧急部署该程序。

以下是将在SEMAC S2（占总量的67%）上部署的固件版本号：670VYJLN

以下是将在SEMAC S3V3（占总量的33%）上部署的固件版本号：628AUYSD

2. 加强监督平台的配置

配置

目的是限制可用于实施攻击的技术要素，只安装必要的服务和设备。

提高安全等级需要采取更严厉的措施，包括：

- 限制平台功能
- 控制平台硬件

A. 更改默认配置

每个组件都按照标准配置，包括：

- 技术账户和相关认证要素
- 使用的网络端口
- 安装和工作目录
- 目录和文件的访问权限
- 用于运行服务或进程的账户，以及与该账户相关的权限
- 安全功能配置文件，尤其是可追溯性。

B. 限制可访问的功能

仅维护对平台运行和安全至关重要的模块，并对其进行适当配置、定期维护和监督。

为此，运营会对平台的技术功能进行分析，以排除已安装但未使用的服务或功能。

每个硬件或软件配置都以参考配置的形式编入清单。

C. 连接元素清单

运营将对构成平台的各个要素进行全面的技术清点。
清单包括可永久或临时连接到平台的实体或远程设备（工作站、服务器、外围设备等）。

如果第三方连接到平台，运营将在清点中注意到这一点，并在风险分析中加以考虑。

D. 使用受控元素

运营直接管理各个要素，包括：

- **部署更新**
- **要素管理**
- 远程配置

分隔

平台遵循分隔逻辑，将每个子系统限制在其行动范围内，以：

- **限制攻**击范围
- **遏制可能的攻**击
- **限制**产生的影响
- **能**够调整每个子系统的安全级别

分隔既适用于物理资源，也适用于逻辑资源。

A. 子系统划分

子系统的划分基于以下标准：

- **功能**
- **数据保**护水平
- **暴露程度**
- **安全等**级

子系统之间的任何连接都必须以功能需求为依据。

B. 物理分隔

一台服务器专用于最关键的应用

C. 逻辑分隔

服务器上存储的所有数据都事先经过加密。 每个子系统都有自己的加密机制。

子系统之间的所有通信都通过经过加密和验证的虚拟专用网络进行。

远程访问

A. 公共访问

公共访问使用HTTPS协议，通过出示服务器证书对平台进行验证。

为平台用户引入双因素认证。

B. 移动访问

对移动工作站进行配置，以与平台建立经过验证和加密的通道。
通道无法停用，无法访问互联网或本地网络。
系统分区和数据分区完全加密

工作站采用双因素认证。

网络过滤

除了分隔之外，还建立过滤机制。

A. 过滤点

子系统之间的相互连接是主要的过滤点，周边过滤和本地过滤都应用于此。

B. 过滤规则

流量矩阵包括现行的过滤规则。 **每年更新**。

C. 实施

专用防火墙根据授权列表原则进行过滤。