台达电子产品安全漏洞说明 **DIAEnergie**
文件编号： Delta-PCSA-2023-00003
日期：2023 年 4 月 20 日
主旨： DIAEnergie 多个漏洞处理说明

This document contains IABG's confidential information that belongs to Delta Electronics, Inc.
Without the prior written consent from Delta, any disclosure or use of this document is prohibited.

1 说明

台达电子产品 DIAEnergie 被通报存在“SQL 注入”、“跨站脚本”，在此针对漏洞的相关分析及处理提出说明。

2 漏洞说明

2.1 受影响的产品

DIAEnergie v1.9.0 及更早的版本

2.2 漏洞概述

2.2.1 SQL 注入 (CWE-89)

主要原因是程序对用户输入数据的合法性没有判断和处理，导致攻击者可以在 Web 应用程序中事先定义好的 SQL 语句中添加额外的 SQL 语句，在管理员不知情的情况下实现非法操作，以此来实现欺骗数据库服务器执行非授权的任意查询，从而进一步获取到数据信息。

此漏洞的 CVE 编号是 CVE-2022-40967、CVE-2022-41133 和 CVE-2022-41773。此漏洞被给定的 CVSS v3 分数 8.8。

2.2.2 跨站脚本 (CWE-79)

跨站脚本攻击（Cross-site scripting，XSS）是一种安全漏洞，攻击者可以利用这种漏洞在网站上注入恶意的客户端代码。若受害者运行这些恶意代码，攻击者就可以突破网站的访问限制并冒充受害者。

此漏洞的 CVE 编号是 CVE-2022-41701、CVE-2022-40965 、CVE-2022-41555、CVE-2022-41702、CVE-2022-41651。此漏洞被给定的 CVSS v3 分数 8.7。

3 风险评估

- 攻击者利用此漏洞，通过从软件之用户接口输入特定的数据，可能导致 “允许任意代码执行”。

Delta Confidential

4 缓解措施

台达电子修补此漏洞，已于 2022 年 10 月 15 日 DIAEnergie 发布内部发行新版补丁 1.9.01.002，请使用者与台达前线处理窗口 SC/FAE 进行索取。

Delta Confidential

This document contains IABG's confidential information that belongs to Delta Electronics, Inc.
Without the prior written consent from Delta, any disclosure or use of this document is prohibited.