江苏江扬电缆有限公司

江扬电缆能源管理平台

弱口令漏洞

1、漏洞详情

发现时间	2024 年 09 月 29 日
单位名称	江苏江扬电缆有限公司
网站名称	江扬电缆能源管理平台
漏洞类型	弱口令漏洞
风险等级	低危
网站域名	http://www.drkjyjdz.com:8888/login?redirect=%2Findex
IP 地址	http://47.116.136.137:8888/

2、漏洞分析

2.1 漏洞简述：

江苏江扬电缆有限公司江扬电缆能源管理平台存在弱口令漏洞，攻击者可利用该漏洞成功进入管理后台，拥有超级管理员权限，进行相应后门留置等机密性、完整性、可用性破坏。

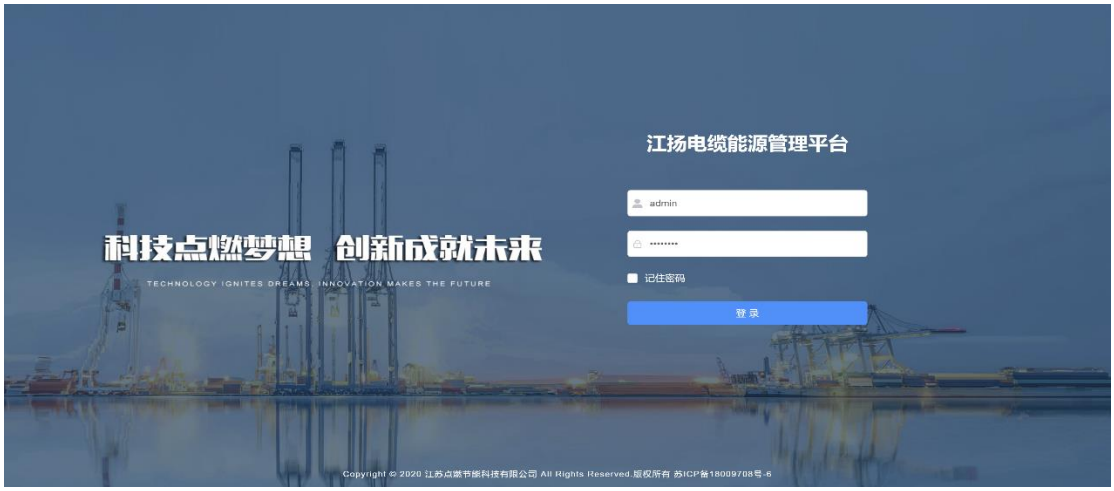
2.2 漏洞 URL

http://47.116.136.137:8888/

2.3 复现步骤

浏览器输入该云平台网址 http://47.116.136.137:8888/，分别填入账号：admin，密码：admin123，如下图所示，即可以超级管理员身份进入该平台。

超级管理员身份拥有最高权限，可进行用户、各部门及业务架构的权限管理、增删改查，并对系统运行情况和日志管理进行监控，篡改。



3、漏洞总结

江苏江扬电缆有限公司江扬电缆能源管理平台存在弱口令漏洞，攻击者可利用该漏洞成功进入管理后台，拥有超级管理员权限，进行相应机密性、完整性、可用性等破坏。

分别填入账号：admin，密码：admin123，如下图所示，即可以超级管理员身份进入该平台。超级管理员身份拥有最高权限，可进行用户、各部门及业务架构的权限管理、增删改查，并对系统运行情况和日志管理进行监控，篡改。

4、修复建议

1、实施强密码策略，要求用户使用包含大小写字母、数字和特殊字符的复杂密码，并设置密码最小长度要求。通过密码策略强制用户创建强密码，增加破解的难度。

2、使用安全的哈希算法对用户密码进行加密，并将加密后的密码存储在数据库中，而不是明文存储。使用加盐哈希算法，如 bcrypt 或 PBKDF2，加强密

码的安全性。

3、引入双因素认证机制，增加登录的安全性。通过使用额外的验证因素，如短信验证码、令牌或生物识别，提高身份验证的可靠性。

4、提醒用户定期更改密码，减少被攻击的风险。通过定期要求用户更改密码，降低弱口令被长期利用的可能性。

5、锁定用户账户和监控异常登录活动，阻止恶意行为。实施账户锁定机制，限制连续失败的登录尝试次数，同时监控异常登录行为，及时发现并采取相应的安全措施。