致远 OA 前台任意用户密码修改漏洞通告

■ **通告编号** **NS-2023-00**	■ 发布日期 **2023-09-12**
■ **漏洞危害** **攻击者利用漏洞可实现任意用户登录**	
■ **TAG** 致远 OA、任意用户登录	

一. 漏洞概述

近日，绿盟科技 CERT 监测到致远 OA 前台任意用户密码修改漏洞，由于用户在修改密码时短信验证码认证存在缺陷，攻击者可以通过构造恶意数据修改任意用户密码，导致任意用户登录，进一步利用可实现远程代码执行。

致远 OA 是一款企业级办公自动化软件，它提供了一系列的办公自动化解决方案，包括文档管理、流程管理、协同办公、知识管理、人力资源管理等功能。致远 OA 可以帮助企业实现信息化管理，提高工作效率和管理水平，同时也可以提高企业的竞争力。

二. 影响范围

受影响版本

- 致远 OA=V5
- 致远 OA=G6
- 致远 OA=V8.1SP2
- 致远 OA=V8.2

三. 漏洞防护

3.1 官方升级

目前官方已发布安全版本修复此漏洞，建议受影响的用户及时升级防护：

https://service.seeyon.com/patchtools/tp.html#/patchList?type=%E5%AE%89%E5%85%A8%E8%A1%A5%E4%B8%81&id=171

声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。

绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。