缺陷编号	漏洞起因	漏洞标题
wooyun-2015-132010	弱口令	工控安全之华润燃气敏感环境竟然未走专线可导致内网渗透（监控/配置/阀门可控未测）
wooyun-2015-129388	注入	华润化工控股有限公司信息门户设置缺陷/sql 注入
wooyun-2015-125651	弱口令	某地有线电视内网沦陷可能修改推送广告内容等
wooyun-2015-125399	注入	中华工控网SQL注入导致全网数据沦陷90W会员数据#打包
wooyun-2015-122677	弱口令	某工控系统配置不当危及船只安全
wooyun-2015-117227	弱口令	某水库工控系统存在弱口令(成功渗透)
wooyun-2015-116558	配置不当	某电厂监管系统缺陷可导致整个工控网络沦陷（DCS/PLC 可被操控执行任何命令）
wooyun-2015-107326	注入	某油田开发公司工控系统sql 注入
wooyun-2015-96729	配置错误	VA 弱密码致华北工控内网远程桌面服务器/内网穿透/涉及敏感信息
wooyun-2014-87708	弱口令	温州市管道燃气公司 SCADA 系统弱口令
wooyun-2014-86726	逻辑漏洞	中国工控网任意用户密码重置漏洞
wooyun-2014-83839	弱口令	大量外网 web 监控系统后台存在弱口令(涉及两款监控产品，涵盖宾馆、车间、仓库、企业内部等)
wooyun-2014-71890	弱口令	某财政信息网系统管理系统密码泄露
wooyun-2014-58681	配置不当	对电厂生产控制网络的一次漫游（针对工控网络的小型APT 攻击）
wooyun-2013-42212	目录遍历	北京市一工控系统多处漏洞可内网渗透（已经发现webshell）
wooyun-2013-22961	网络未授权访问	301 基础设施系列-国外基础设施 1（鲍里斯波尔国际机场地面照明控制和监测系统）暴漏
wooyun-2013-21848	弱口令	从对某电厂 DCS 控制系统的实体控制续谈工控安全（可控制电厂实体设备）
wooyun-2013-21314	弱口令	从某知名厂商 MIS 软件逻辑缺陷谈对某工控网络的渗透 第二份案例ops.wooyun.org
wooyun-2013-21250	弱口令	从某知名厂商 MIS 软件逻辑缺陷谈对某工控网络的渗透
wooyun-2012-16328	未授权访问	美国一工业操作系统越权访问,可控制能源基础设施
wooyun-2012-10818	弱口令	武汉市某工控系统弱口令导致信息泄漏，企业各种记录在内
wooyun-2012-09565	命令执行	放统计代码，站长一秒钟变 APT 攻击专家（wooyun-2012-09025 续）
wooyun-2012-09025	设计缺陷	UC 云端加速引擎存在非正常泄露referer 问题
wooyun-2012-07340	账户体系控制不严	某省级能源集团旗下XX 存在安全隐患
wooyun-2012-07172	配置错误	某环境集成平台存在严重问题！获得客户端控制实权！
wooyun-2012-07084	弱口令	中国电信某 GPS 监控平台存在严重问题
wooyun-2012-06997	SQL注入	天津鑫然智能 DCS 监控平台
wooyun-2012-06196	配置不当	国内某大型风电工控系统应用配置失误
wooyun-2012-04702	信息泄露	南京国电自动化股份有限公司厂站监控系统源代码及配置文件泄露漏洞
wooyun-2014-84258	未授权访问	丹堰市自来水公司 SCADA 管网综合监测系统漏洞
wooyun-2014-80994	注入	哈药集团分公司sql 注入(影响大量同服网站数据库)
wooyun-2014-58654	命令执行	CenturyStar9.0 SCADA 组态软件存在远程命令执行漏洞

		任命令执行漏洞
wooyun-2014-58130	上传漏洞	某电厂 SCADA 测试文件未清理存在任意上传漏洞(可导致服务器沦陷)
wooyun-2013-34711	弱口令	天能集团某 SCADA 系统弱口令登陆
wooyun-2013-21086	SQL注入	某煤矿 SCADA 系统存在严重缺陷可导致服务器沦陷
wooyun-2012-07334	未授权访问	某市燃气管道 SCADA 系统登录绕过
wooyun-2012-06952	设计缺陷	某 SCADA 电力监控系统漏洞