工业控制系统信息安全风险提示

2016年第2期（总第7期）　　2016年3月14日

工业控制设备默认密码清单被公布
我国工业企业需加强核查与管理

2015年12月17日，俄罗斯某工控安全研究团队通过互联网公布了名为“SCADAPass”的工业控制设备默认密码清单，[illegible]2016年2月1日[illegible]，施耐德等国内外48个厂商的134个工控设备型号，详细描述了各工控设备的设备类型、默认用户名及密码等敏感信息。黑客可能利用该清单获取的默认密码，通过[illegible]登录（web）、远程登录（Telnet、FTP）、厂商专用终端登录等方式获取工控设备的操作权限，实施修改系统设置、执行root命令、替换系统固件、非法控制等攻击。根据统计，清单所涉及的部分工控设备应用于我国重要工控系统，我国工业控制系统运营单位及相关主管部门需引起高度重视。

建议工业控制系统运营单位结合自身情况，及时采取以下核查与管理措施：1.通过运营单位工控系统软硬件资产清

单与“SCADAPass”清单的对比核查，梳理出受默认密码风险影响的工控设备；2.修改工控设备默认密码并强化用户密码；3.断开工控设备不必要的公网连接，关闭工控设备的HTTP/Telnet/FTP/SSH等不必要的传统网络服务；4.部署其它辅助的访问控制和安全认证措施。

编制单位：工业和信息化部电子科学技术情报研究所

发送：各地工业和信息化部主管部门、有关国有大型企业、有关工业控制系统厂商

抄送：工业和信息化部信息化和软件服务业司

（联系人：李耀兵 010-88683438）