

B78
2016年3月29日收

工业控制系统信息安全 风险提示

工业和信息化部 公安部 国家安全部 工业和信息化部 公安部 国家安全部

工业和信息化部 公安部 国家安全部 工业和信息化部 公安部 国家安全部

工业和信息化部 公安部 国家安全部 工业和信息化部 公安部 国家安全部

工业和信息化部 公安部 国家安全部 工业和信息化部 公安部 国家安全部

工业和信息化部 公安部 国家安全部 工业和信息化部 公安部 国家安全部

单与“SCADAPass”清单的对比核查，梳理出受默认密码影响、
易受攻击的工控设备；2. 修改工控设备默认密码并强化用户密
码策略；3. 关闭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)