宁 夏 回 族 自 治 区

经济和信息化委员会文件

宁经信产信发〔2018〕187 号

自治区经济和信息化委员会关于做好施耐德工业控制软件、横河电机 STARDOM 控制器高危漏洞风险防范的通知

五市工信局、宁东能源化工基地管委会经发局、银川经济技术开发区管委会经发局，有关企业：

根据宁夏网络安全通报中心《关于施耐德工业控制软件存在高危漏洞直接影响关键制造业和能源行业网络安全的紧急预警通报》（第 129 期）、《关于横河电机 STARDOM 控制器存在高危漏洞的紧急预警通报》（第 130 期），为确保工控系统安全运行，有效防范我区采用施耐德工业控制软件、横河电机 STARDOM 控制器的

工业控制系统受到漏洞影响，对可能演变为严重事件的情况，及时采取应对措施，避免出现网络安全事故。现将具体情况通知如下：

一、漏洞分析

（一）施耐德工业控制软件。

施耐德旗下产品 U.motion builder 存在的远程代码执行（RCE）漏洞编号为 CVE-2018-7784、CVE-2018-7785，安全评级为“高危”。U.motion 是一款自动化构建解决方案，用于全球商业设施、关键制造业和能源行业。U.motion builder 工具能让用户为自己的 U.motion 设备创建项目。

漏洞一（CVE-2018-7784）：程序对提交的数据过滤不严，导致输入的数据被当作代码执行。通过漏洞，攻击者可以在存在漏洞的机器上远程执行任意代码、泄漏信息或者引发程序报错。

漏洞二（CVE-2018-7785）：远程命令注入漏洞，攻击者可以在无需认证的情况下，对存在漏洞的主机执行任意远程命令。

（二）横河电机 STARDOM 控制器。

横河电机 STARDOM 控制器存在的高危漏洞编号为 CVE-2018-10592,安全级别为“高危”。该漏洞源于控制器存在一个硬编码的用户名和密码凭证，具有网络访问权限的攻击者可借此登录设备并执行系统命令，攻击者利用该漏洞可以对 STARDOM 控制器发起远程攻击，并执行任意代码，获取控制器所有权限。

二、影响范围

1.施耐德旗下产品 U.motion builder 存在的漏洞影响 U.motion server 1.3.4 及以下版本。

2.日本横河电机 STARDOM 多款控制器，官方发布受影响控制器有 FCJ（R4.02 and prior）、FCN-100(R4.02 and prior)、FCN-RTU(R4.02 and prior)、FCN-500(R4.02 and prior)。由于 STARDOM 控制器应用十分广泛，涉及能源、关键制造、食品和农业等行业，可造成严重危害。

三、相关对策

（一）积极开展漏洞修复工作。目前，施耐德、横河电机官方已经发布补丁对漏洞进行修复，各地工信部门要督促有关企业做好补丁离线测试和修复工作,确保我区工控系统安全稳定运行。

（二）认真组织开展自查工作。为了防止漏洞被远程利用，各地工信部门要督促本地区工业企业严格《工业控制系统信息安全防护指南》要求，开展工业控制系统及工控主机的安全防护工作。一是做好安全配置，定期进行配置审计；二是通过边界防护设备对工控网络与企业网或互联网的边界进行安全防护；三是强化登录账户及密码，避免弱口令；四是关闭不必要的 HTTP、FTP、TELNET 等高风险服务。

四、补丁下载地址

1.施耐德官方网站补丁下载地址：

https://www.schneider-electric.com/en/download/document/Umotion_Server_update/。

2.横河电机官方网站补丁下载地址：

https://www.securityweek.com/hardcoded-credentials-expose-yokogawa-controllers-attacks。

联系人：齐伟，联系电话：6038361。

宁夏回族自治区经济和信息化委员会

2018年6月12日

（此件公开发布）

宁夏回族自治区经济和信息化委员会办公室　　2018年6月12日印发