

河南省教育信息安全监测中心
关于做好公共电子显示屏、重点网站等网络
安全保障，严防发生涉政网络安全事件的
风险提示



关于做好公共电子显示屏、重点网站等网络安全保障，严防发生涉政网络安全事件的风险提示

事件描述

接有关部门通报，广东和丰自动化科技有限公司产品“和丰数字标牌”电子屏联网控制系统存在高危漏洞，攻击者可利用该漏洞对有关电子屏实施内容篡改。

请各单位高度重视，立即排查本单位“和丰数字标牌”电子屏联网控制系统使用情况，建议在官方修复措施发布前，充分研判工作需要，尽量避免联网使用，严防网络攻击篡改导致现实危害。

安全建议

关注厂家重要通知和软件升级动态，保持软件为最新版本，截至至 2024 年 2 月 22 日官方发布软件最新版本号列举如下，请务必升级：

云服务发布平台：HF-V3.0.0.2024022201

多媒体信息发布系统：HF-V3.0.1.2024022201

多媒体触摸查询系统：HF-V3.0.2.2024022201

多媒体信息发布系统旗舰版：HF-V3.0.3.2024022201

更多相关信息请访问厂家官网：<https://www.howfor.com>

风险提示

公共电子显示屏、网站遭攻击篡改风险较高，且此类设施遭攻击篡改极易转化为政治安全事件。2023年国庆期间，境外黑客组织攻击篡改我境内多地公共电子显示屏和多个网站页面，张贴反宣信息，造成恶劣影响。2024年春节期间，境外黑客组织扬言对我境内公共电子显示屏等目标实施攻击，企图进行滋扰破坏，被及时发现并予以防范应对。

全国“两会”召开在即，请各单位高度重视，加强安全监测，严密防范境外敌对势力网络攻击破坏，做好应急处突准备，完善应急预案，将处置应对境外敌对势力攻击篡改公共电子显示屏、网站作为重点内容，发生重大网络安全事件要迅速妥善处置并报告。

联系方式

地址：河南省郑州市二七区大学路75号郑州大学南校区逸夫楼

电话：0371-67761893、0371-67765016

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052