经监测，潍坊市所属网站“安丘市人民医院网站”（tj.aqsrmyy.com）存在越权访问漏洞，如不采取紧急处置措施，攻击者获取网站配置信息，可能导致“一般”级别网络安全事件（附件1）。

请你单位迅速组织开展调查处置工作，核实漏洞影响及危害程度，督促相关单位落实党委（党组）网络安全工作责任制要求，处置情况请按《网络安全事件和隐患处置情况反馈表》要求填写，加盖公章，将电子版、纸质扫描件于11月25日反馈swwxbwak@wf.shandong.cn

附件：1. 预警信息

2. 网络安全事件和隐患处置情况反馈表

|  |
| --- |
| 抄送：省公安厅、省安全厅、省保密局、省大数据局，潍坊市卫生健康委。 |

附件1

预警信息

|  |  |  |  |
| --- | --- | --- | --- |
| 类别 | 网络安全风险隐患 | | |
| 警示事项 | 潍坊市所属网站“安丘市人民医院网站”（tj.aqsrmyy.com）存在越权访问漏洞，如不采取紧急处置措施，攻击者获取网站配置信息，可能导致“一般”级别网络安全事件。 | | |
| 预警等级 | **蓝色** | | |
| 详情 | **漏洞地址：**  http://tj.aqsrmyy.com:15672/cli/rabbitmqadmin  越权访问漏洞 | | |
| 可能影响 | 信息泄露、网页篡改 | | |
| 应采取措施 | 修复该漏洞，调查漏洞发生原因并整改 | 时限要求 | 2个工作日 |

附件2

网络安全事件和隐患处置情况反馈表

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| \*事件名称 | |  | | | | | | | | |
| \*事件类型 | |  | | | \*危害等级 | | | 低危、中危、高危或紧急 | | |
| \*事件描述 | |  | | | | | | | | |
| \*相关网站或信息系统名称 | |  | | | \*IP地址 | | |  | | |
| \*专线接入服务商 | |  | | | 接入时间 | | |  | | |
| \*域名URL | |  | | #域名注册商 |  | | | #域名注册时间 | |  |
| \*是否等保 | |  | | #等保级别 |  | | | #等保备案号 | |  |
| \*隶属单位 | |  | | \*系统承建单位 |  | | | \*安全运营服务商 | |  |
| \*负责人 | |  | | \*联系电话 |  | | | \*联系邮箱 | |  |
| \*处置人 | |  | | \*联系电话 |  | | | \*联系邮箱 | |  |
| 总  结  报  告 | \*事件发生原因 |  | | | | | | | | |
| \*事件经过及处理 |  | | | | | | | | |
| \*今后防  范措施 |  | | | | | | | | |
| \*网站是否恢复正常 | |  | | | | \*网站恢复时间 | |  | |
| 是否保留或  发现作案软件 | |  | | | | 是否有网站日志 | |  | |
| 网络安全分管领导：（签字）  涉事单位：（盖章） | | | | | | 地市网信部门：（盖章） | | | | |

注：\*为必填项；#可与前一项同为空。