lgb

**安全评估报告**

|  |  |
| --- | --- |
| **评估项目** | **是否包含** |
| 合规性评估 | 含 |
| 资产评估 | 含 |
| 流量评估 | 含 |
| 无线评估 | 含 |
| 恶意代码核查 | 含 |
| 主机配置核查 | 含 |

lgb

2023年05月26日

# 评估对象信息

## 企业信息

|  |  |
| --- | --- |
| 企业名称 | lgb |
| 所属省市区 |  |
| 所属行业 |  |

## 1.2.任务信息

|  |  |  |  |
| --- | --- | --- | --- |
| 任务名称 | | | lgb |
| 责任相关方 | | 系统集成商 |  |
| 运维单位 |  |
| 投运时间 | | | 2023-05-24 |
| 服务对象 | | | 单位内部人员 |
| 服务范围 | | | 全国 |
| 区域名称 | | | 区域一,区域三,区域二 |
| 数据存储方式 | | | 本地存储 |
| 年存储数据量级 | | | 0 |
| 联网情况 | 互联网连接 | | 否 |
| 办公网连接 | | 否 |
| 其他系统 | | 否 |

## 1.3资产总览

## 1.3.1**资产类型统计**

#### 1.3.1.1资产类别总览

|  |  |  |
| --- | --- | --- |
| **资产类型** | **资产数量** | **占比** |
| 数据服务器（DB） | 7 | 43.75% |
| 网络摄像机（IP Camera） | 2 | 12.5% |
| 网络视频录像机（NVR） | 1 | 6.25% |
| 其他设备（other） | 6.0 | 37.5% |

# 评估结果详情

## 合规性评估

### 合规性分析结果

|  |  |  |
| --- | --- | --- |
| 分析结果 | 评定等级 | 评定等级：一级 |
| 评估结果 | 评定结果：未达标 |
| 分析依据 | | 本套合规性检查标准根据《信息安全等级保护基本要求 第5部分：工业控制系统安全扩展要求》进行整理制订。 |
| 不通过项数 | | 7项 |
| 不适用项数 | | 0项 |

### 合规性评估整改建议

| **评估范围** | **评估内容** | **评估项** | **整改建议** |
| --- | --- | --- | --- |
| 安全物理环境 | 物理访问控制 | 机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。 |  |
| 安全物理环境 | 物理访问控制 | 机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。 |  |
| 安全物理环境 | 防盗窃和防破坏 | 应将设备或主要部件进行固定，并设置明显的不易除去的标记； |  |
| 安全物理环境 | 防雷击 | 应将各类机柜、设施和设备等通过接地系统安全接地； |  |
| 安全物理环境 | 防火 | 机房应设置灭火设备。 |  |
| 安全物理环境 | 防水和防潮 | 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； |  |
| 安全物理环境 | 温湿度控制 | 应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。 |  |
| 安全物理环境 | 电力供应 | 应在机房供电线路上配置稳压器和过电压防护设备； |  |

## 资产安全评估

通过资产安全评估模块对被测单位核心工控资产、网络及安全设备、工程师站及操作员站等资产进行评估分析，内容包括资产端口信息、资产威胁信息、工控系统漏洞信息和操作系统漏洞信息。

### 端口统计信息

本次资产评估共检查56台设备，有40台存在端口开放，开放端口52种，共计161个。

设备占比：开放此端口的设备数量占被检查设备总数量之比。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **端口** | **服务** | **数量** | **设备占比** |
| 1 | 137 | netbios-ns | 19 | 11.80% |
| 2 | 139 | netbios-ssn | 18 | 11.18% |
| 3 | 445 | SmbOSDiscovery | 16 | 9.94% |
| 4 | 22 | ssh | 10 | 6.21% |
| 5 | 80 | http | 9 | 5.59% |
| 6 | 3306 | mysql | 9 | 5.59% |
| 7 | 443 | https | 6 | 3.73% |
| 8 | 443 | vmware | 6 | 3.73% |
| 9 | 8000 | http-alt | 4 | 2.48% |
| 10 | 8083 | us-srv | 4 | 2.48% |
| 11 | 6000 | X11 | 4 | 2.48% |
| 12 | 445 | microsoft-ds | 4 | 2.48% |
| 13 | 3389 | ms-wbt-server | 3 | 1.86% |
| 14 | 3702 | onvif | 2 | 1.24% |
| 15 | 554 | rtsp | 2 | 1.24% |
| 16 | 3389 | rdp | 2 | 1.24% |
| 17 | 102 | S7; IEC61850 | 2 | 1.24% |
| 18 | 7000 | afs3-fileserver | 2 | 1.24% |
| 19 | 4840 | opcua-tcp | 2 | 1.24% |
| 20 | 84 | ctf | 2 | 1.24% |
| 21 | 23 | telnet | 2 | 1.24% |
| 22 | 10001 | scp-config | 2 | 1.24% |
| 23 | 5900 | vnc | 2 | 1.24% |
| 24 | 1433 | ms-sql-s | 1 | 0.62% |
| 25 | 81 | hosts2-ns | 1 | 0.62% |
| 26 | 8086 | d-s-n | 1 | 0.62% |
| 27 | 9200 | wap-wsp | 1 | 0.62% |
| 28 | 1521 | oracle | 1 | 0.62% |
| 29 | 8080 | http-proxy | 1 | 0.62% |
| 30 | 5432 | pgsql | 1 | 0.62% |
| 31 | 5432 | postgresql | 1 | 0.62% |
| 32 | 7314 | swx | 1 | 0.62% |
| 33 | 20000 | DNP3 | 1 | 0.62% |
| 34 | 515 | printer | 1 | 0.62% |
| 35 | 6379 | redis | 1 | 0.62% |
| 36 | 123 | ntp | 1 | 0.62% |
| 37 | 11 | systat | 1 | 0.62% |
| 38 | 12288 | unknown | 1 | 0.62% |
| 39 | 8085 | unknown | 1 | 0.62% |
| 40 | 79 | finger | 1 | 0.62% |
| 41 | 50000 | ibm-db2 | 1 | 0.62% |
| 42 | 8090 | opsmessaging | 1 | 0.62% |
| 43 | 86 | mfcobol | 1 | 0.62% |
| 44 | 2006 | invokator | 1 | 0.62% |
| 45 | 1723 | pptp | 1 | 0.62% |
| 46 | 7001 | afs3-callback | 1 | 0.62% |
| 47 | 37810 | dahua-udp | 1 | 0.62% |
| 48 | 683 | corba-iiop | 1 | 0.62% |
| 49 | 491 | go-login | 1 | 0.62% |
| 50 | 111 | rpc | 1 | 0.62% |
| 51 | 37777 | unknown | 1 | 0.62% |
| 52 | 3702 | ws-discovery | 1 | 0.62% |

### 端口开启设备

|  |  |  |
| --- | --- | --- |
| **区域** | **设备IP** | **开放端口** |
| 区域一 | 192.168.5.195 | 7001,139,102,445,3389,4840,137 |
| 区域一 | 192.168.5.197 | 23,111,22 |
| 区域一 | 192.168.5.192 | 139,80,3306,445 |
| 区域一 | 192.168.5.236 | 137,6000,445,139 |
| 区域一 | 192.168.5.159 | 139,102,445,443,80,10001,137,81 |
| 区域一 | 192.168.5.115 | 10001,443,139,137,445 |
| 区域一 | 192.168.5.232 | 443,445,137,139 |
| 区域一 | 192.168.5.199 | 3389,445 |
| 区域一 | 192.168.5.77 | 3306,139,137,443,445,6000 |
| 区域一 | 192.168.5.229 | 139,445,5900,137,443 |
| 区域一 | 192.168.5.186 | 445,139 |
| 区域一 | 192.168.5.103 | 80,5432,443,22 |
| 区域一 | 192.168.5.105 | 445,139,11,137,86,79,515 |
| 区域一 | 192.168.5.149 | 139,445,137 |
| 区域一 | 192.168.5.220 | 22 |
| 区域一 | 192.168.5.100 | 139,137,445,3389,443 |
| 区域一 | 192.168.5.24 | 37810,8086,37777,3702,554,80 |
| 区域一 | 192.168.5.217 | 137 |
| 区域一 | 192.168.5.219 | 6000,443,445 |
| 区域一 | 192.168.5.250 | 443,80,445,3389,5432,139,137 |
| 区域一 | 192.168.5.251 | 139,3306,445,443,137,6379 |
| 区域一 | 192.168.5.174 | 8000 |
| 区域一 | 192.168.5.175 | 137,139,445 |
| 区域一 | 192.168.5.170 | 2006,123,3306,22,9200,8090,683,8083,7000,7314,50000,1521,12288,3702,8085 |
| 区域一 | 192.168.5.214 | 22,5900 |
| 区域一 | 192.168.5.215 | 3306 |
| 区域一 | 192.168.5.176 | 8083,22 |
| 区域一 | 192.168.5.2 | 80,1723,443,84 |
| 区域一 | 192.168.5.133 | 8083,22,84,491,3306,1433 |
| 区域一 | 192.168.5.1 | 80,443 |
| 区域一 | 192.168.5.208 | 137 |
| 区域一 | 192.168.5.162 | 139,445,137,3306 |
| 区域一 | 192.168.5.164 | 139,7000,445,8000,137 |
| 区域一 | 192.168.5.169 | 137,3306 |
| 区域一 | 192.168.5.249 | 22,80,23,8080 |
| 区域一 | 192.168.5.124 | 20000,22,8083,4840 |
| 区域一 | 192.168.5.88 | 3389,8000 |
| 区域一 | 192.168.5.119 | 3306 |
| 区域一 | 192.168.5.41 | 139,137,445,6000 |
| 区域一 | 192.168.7.40 | 3702,8000,22,554,80 |

### 疑似跨区连接

### 资产漏洞信息

本次评估通过无损扫描整理出漏洞8339个。

其中危急463个，高危3630个，中危3770个，低危476个。

各个区域的漏洞情况为:区域一有危急463个,高危3630个,中危3770个,低危476个。

本次评估共对台设备的漏洞无损扫描，其中漏洞数前10位的设备为：

#### 工控系统漏洞信息

本次评估通过无损扫描整理出的工控系统的漏洞有50个。

其中危急8个，高危26个，中危14个，低危2个。

根据本次评估所扫描出来的漏洞，工控系统漏洞评分整理排名前10位的为

| **序号** | **漏洞等级** | **漏洞编号** | **漏洞名称** | **影响厂商** | **影响IP** | **区域** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 低危 | CVE-2022-32296 | Linux kernel 安全漏洞 |  | 192.168.5.214,192.168.7.40,192.168.5.220,192.168.5.2,192.168.5.176,192.168.5.133 | 区域一 |
| 2 | 低危 | CVE-2022-33981 | Linux kernel 资源管理错误漏洞 |  | 192.168.5.214,192.168.7.40,192.168.5.220,192.168.5.2,192.168.5.176,192.168.5.133 | 区域一 |
| 3 | 中危 | CVE-2022-0494 | Linux kernel 信息泄露漏洞 |  | 192.168.5.214,192.168.7.40,192.168.5.220,192.168.5.2,192.168.5.176,192.168.5.133 | 区域一 |
| 4 | 中危 | CVE-2021-20317 | Linux kernel 安全漏洞 |  | 192.168.5.214,192.168.7.40,192.168.5.220,192.168.5.2,192.168.5.176,192.168.5.133 | 区域一 |
| 5 | 中危 | CVE-2010-1138 | VMware 虚拟网络堆栈远程攻击敏感信息泄露漏洞 | VMware | 192.168.5.77,192.168.5.229,192.168.5.219,192.168.5.115,192.168.5.100,192.168.5.232 | 区域一 |
| 6 | 中危 | CVE-2019-1125 | Intel x86-64 CPU 信息泄露漏洞 |  | 192.168.5.162,192.168.5.195,192.168.5.250,192.168.5.251,192.168.5.186,192.168.5.175,192.168.5.192,192.168.5.236,192.168.5.115,192.168.5.159,192.168.5.105,192.168.5.149,192.168.5.100,192.168.5.232,192.168.5.199,192.168.5.77,192.168.5.217,192.168.5.229,192.168.5.219,192.168.5.41 | 区域一 |
| 7 | 中危 | CVE-2022-1016 | Linux kernel 缓冲区错误漏洞 |  | 192.168.5.214,192.168.7.40,192.168.5.220,192.168.5.2,192.168.5.176,192.168.5.133 | 区域一 |
| 8 | 中危 | CVE-2022-2380 | Linux kernel 缓冲区错误漏洞 |  | 192.168.5.214,192.168.7.40,192.168.5.220,192.168.5.2,192.168.5.176,192.168.5.133 | 区域一 |
| 9 | 中危 | CVE-2021-4149 | Linux kernel 竞争条件问题漏洞 |  | 192.168.5.214,192.168.7.40,192.168.5.220,192.168.5.2,192.168.5.176,192.168.5.133 | 区域一 |
| 10 | 中危 | CVE-2022-1198 | Linux kernel 资源管理错误漏洞 |  | 192.168.5.214,192.168.7.40,192.168.5.220,192.168.5.2,192.168.5.176,192.168.5.133 | 区域一 |

本次评估对工控漏洞的扫描中，漏洞数前10位的设备为：

#### 操作系统漏洞信息

本次评估通过无损扫描整理出的操作系统的漏洞有3826个。

其中危急167个，高危1878个，中危1593个，低危188个。

根据本次评估所扫描出来的漏洞，操作系统漏洞评分整理排名前10位的为

| **序号** | **漏洞等级** | **漏洞编号** | **漏洞名称** | **影响厂商** | **影响IP** | **区域** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 低危 | CVE-2012-2313 | Linux Kernel ‘rio\_ioctl’ 函数权限许可和访问控制问题漏洞 |  | 192.168.5.214,192.168.7.40,192.168.5.220,192.168.5.2,192.168.5.176,192.168.5.133 | 区域一 |
| 2 | 低危 | CVE-2013-1502 | Oracle MySQL 未明安全漏洞 | 甲骨文 | 192.168.5.162,192.168.5.169 | 区域一 |
| 3 | 低危 | CVE-2014-1444 | Linux kernel‘fst\_get\_iface’函数资源管理错误漏洞 |  | 192.168.5.214,192.168.7.40,192.168.5.220,192.168.5.2,192.168.5.176,192.168.5.133 | 区域一 |
| 4 | 低危 | CVE-2012-0075 | Oracle MySQL 远程未明细节安全漏洞 | 甲骨文 | 192.168.5.162,192.168.5.169 | 区域一 |
| 5 | 低危 | CVE-2016-0609 | Oracle MySQL Privileges组件拒绝服务漏洞 | 甲骨文 | 192.168.5.162,192.168.5.169 | 区域一 |
| 6 | 低危 | CVE-2015-0498 | Oracle MySQL Server Server:Replication子组件拒绝服务漏洞 | 甲骨文 | 192.168.5.162,192.168.5.169 | 区域一 |
| 7 | 低危 | CVE-2015-4792 | Oracle MySQL Server Server : Partition子组件拒绝服务漏洞 | 甲骨文 | 192.168.5.162,192.168.5.169 | 区域一 |
| 8 | 低危 | CVE-2015-4767 | Oracle MySQL Server 远程安全漏洞 | 甲骨文 | 192.168.5.162,192.168.5.169 | 区域一 |
| 9 | 低危 | CVE-2012-0494 | Oracle MySQL Server本地拒绝服务漏洞 | 甲骨文 | 192.168.5.162,192.168.5.169 | 区域一 |
| 10 | 低危 | CVE-2012-0174 | Microsoft Windows 'tcpip.sys'信息泄露漏洞 | RedisLabs | 192.168.5.251,192.168.5.199,192.168.5.41 | 区域一 |

本次评估对操作系统漏洞的扫描中漏洞数前10位的设备为：

## 流量评估

本次流量评估共截取16段,其中区域一截取16段,共计42分15秒。

### 评估结果

| **区域** | **截取时长** | **数据大小** | **协议数量** | **IP**  **数量** | **异常数据包** | **诊断报警数** | **异常警报数** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 区域一 | 2535.0 | 2.41GB | 8 | 2814 | 618358 | 2164598 | 23 |

### 时间流速统计

### 2.3.3数据包大小统计（大包、小包、其他，以个数统计）

在流量评估中截取到数据包共计3170661个,其中区域一 3170661个,其中，截取到大包数据（＞1518的数据包）共计0个,其中区域一 0个,其中，截取到小包数据（<60的数据包）共计618358个, 其中区域一 618358个,

### 2.3.4诊断报警统计

在流量评估中,共发生诊断报警2164598次，其中区域一区 2164598次。

诊断报警详情统计如下。

### 2.3.5 诊断报警整改建议

|  |  |  |
| --- | --- | --- |
| 诊断报警名称 | 发生次数 | 整改建议 |
| ARP请求风暴 | 172 | 1、使用防病毒软件查杀发送ARP数据包的主机；2、关闭发送ARP数据包的扫描软件；3、设置好镜像操作并将系统安装在连接镜像端口的主机上。 |
| ICMP端口不可达 | 7296 | 1、打开该服务对应的端口2、检查该服务的配置，重启服务；3、打开防火墙或路由器上该端口的访问控制策略。 |
| IP非法校验 | 941495 | 1、传输线路电磁干扰太大或某个设备存在故障。 |
| TCP端口扫描 | 16369 | 1、检查源主机是否感觉蠕虫病毒；2、检查源主机是否存在人为扫描攻击。 |
| TCP连接被拒绝 | 6718 | 1、在服务器上打开该服务对应的端口；2、检查服务器上运行状态。 |
| TCP连接重复的连接尝试 | 23372 | 1、确定服务器是真实存在以及是否开机；2、打开服务器该服务对应的端口3、在防火墙上打开该访问控制策略。 |
| TCP重传数据包 | 530447 | 1、检查网络中运行的服务，检查或更换网络的软硬件配置；2、检查交换机或路由器的工作状态；3、更改路由器中的路由配置；4、检查接收端主机的工作状态。 |
| TCP重复确认 | 638729 | 1、检查网络是否存在拥塞。2、检查网络是否由于其他原因导致丢包。3、检查TCP连接的两端主机是否正常。 |

### 2.3.6异常警报统计

此次评估共发现23次异常警报。区域分布如下：

规则警报次数如下：

| **规则名称** | **警报次数** |
| --- | --- |
| IGSS SCADA Delete Function Buffer Overflow | 23 |

### 2.3.7异常警报整改建议

异常警报疑似触发工控病毒行为，建议联系专业的工控安全厂商进行进一步深入检测，以确定病毒行为目的，及发现和定位病毒源。同时，可于评估对象网络中部署工控监测审计类工具，以帮助用户在第一时间发现工控病毒传播行为。也可于工控系统关键节点部署智能保护类工具，以防止并阻断工控病毒的传播感染，进一步保障工业控制系统的安全性。

## 2.4 无线wifi评估

本次无线评估，共扫描2个无线域1,发现无线热点0个,隐藏无线热点0个,弱密码无线热点0个,开启WPS无线热点0个。 123213,发现无线热点0个,隐藏无线热点0个,弱密码无线热点0个,开启WPS无线热点0个。

## 2.5主机设备评估

本次评估共检查56台设备, 其中可做主机设备评估检查的设备为31台。其中,区域一区 31台; 截至报告生成时，实际执行主机设备评估0台，其中，区域一区0台（Windows操作系统设备：0台，Linux操作系统设备：0台）;

### 2.5.1 核查结果

### 2.5.2 修改建议

## 2.6恶意代码评估

本次评估共检查56台设备，执行恶意代码评估的设备有0台，共发现0个恶意代码感染文件，发现时间最近的10笔展示如下，详情参看附件。

# 总结与建议

本次评估，通过“合规性评估”“资产评估”“流量评估”“无线评估”“主机设备评估”“恶意代码评估”发现了被检测单位存在的风险状况。根据相关安全标准和组织自身的安全要求，请酌情制定相应的安全控制规范，执行相应的控制措施，以达到防范威胁，减少自身脆弱性，将风险降低到可接受范围内的目的，保障评估对象系统安全。

附件：[lgb安全评估报告-20230526132403.xlsx](.\lgb安全评估报告-20230526132403.xlsx)