# 江苏电信业务网安全管理中心

**漏洞扫描能力输出文档**

修订版本：

编写单位：

2017年08月

## 一．文档说明

江苏电信业务网安全管理中心（以下简称“业务网”）以WebService服务接口形式对第三方提供扫描能力（漏洞、端口、WEB）输出。

该接口实现了创建扫描任务，获取任务状态、获取扫描报告、及获取任务详情信息等需求。此外，接口还提供了获取扫描器信息和邮件通知的能力。

## 二．接口介绍

1. 服务接口地址

http://132.228.5.101:6060/soc/socAlarm/openScan?wsdl

1. 服务接口类型

WebService / JAX-WS / SOAP

1. 协议报文载体

XML文本

## 三．接口能力

1. 创建扫描任务
   1. 接口：public void createScanTask(List<TaskItem> scanTasks)
   2. 参数：

TaskItem: {

String uuid; //识别ID

String taskName; //任务名称，在列表中不可重复

int deviceId; //设备ID，设备信息由getScannerInfo接口获取

String targets; //扫描目标，例如：192.168.1.100-123,192.168.1.200

int scanType; //扫描类型：0-端扫、1-漏扫、2-WEB

int reportType; //报告类型：1-html、2-word、3-pdf、4-excel、5-不生成

String scanTime; //执行时间，yyyy-MM-dd-HH:mm，空为立即执行

}

* 1. 返回：

1. 获取任务状态
   1. 接口：public TaskSatus getTaskStatus(String uuid)
   2. 参数：uuid 任务识别ID
   3. 返回：

TaskStatus: {

String uuid; //识别ID

String taskName; //任务名称

int scanStatus; //扫描状态：-1-创建失败,，0-创建成功，1-扫描中，2-扫描完成，3-扫描失败，4-任务暂停，5-异常状态，6-任务不存在

int reportStatus; //报告状态：0-未生成，1-已生成，2-无报告，3-异常状态

int detailStatus; //告警详情状态：0-未生成，1-已生成，2-异常状态

String scanMsg; //扫描状态描述信息

}

1. 获取任务扫描（告警）详情
   1. 接口：public ScanDetail getTaskScanDetail(String uuid)
   2. 参数：uuid 任务识别ID
   3. 返回：

ScanDetail: {

String uuid; //识别ID

String taskName; //任务名称

int scanType; //扫描类型：0-端扫，1-漏扫，2-WEB

List<VulnDetail> details; //告警详情列表

}

VulnDetail: {

String source; //事件源（IP）

String vulnName; //告警名称

String vulnType; //告警类型

String protocol; //网络协议

int port; //端口

String riskLevel; //风险级别

String description; //事件描述

String solution; //解决方案

String startTime; //开始时间

String endTime; //结束时间

}

1. 获取扫描报告
   1. 接口：public ScanReport getTaskScanReport(String uuid)
   2. 参数：uuid 任务识别ID
   3. 返回：

ScanReport: {

String uuid; //识别ID

String taskName; //任务名称

int reportType; //报告类型：1-html、2-word、3-pdf、4-excel、5-不生成

int reportStatus; //报告状态：0-未生成，1-已生成，2-无报告

byte[] data; //报告（zip）文件二进制数据

}

1. 获取扫描器信息
   1. 接口：public SannerInfo getScannerInfo()
   2. 参数：
   3. 返回：

ScannerInfo: {

List<ScannerItem> scanners; //扫描器列表

}

ScannerItem: {

int deviceId; //扫描器ID

String name; //扫描器名称

String deviceType; //扫描器类型

String location; //网络覆盖位置：公网、DCN网、

String description; //描述信息

}

1. 邮件通知
   1. 接口public void sendNotifyMail(MailMessage message)
   2. 参数：

MailMessage: {

List<String> receivers; //收件人列表

String title; //邮件标题

String content; //消息内容

AttachmentItem attachment; //附件内容

}

AttachmentItem: {

String name; //附件名称

byte[] data; //二进制数据

}

* 1. 返回

1. 心跳监测
   1. 接口：public int getHeartBeat()
   2. 参数：
   3. 返回：0-正常
2. 获取扫描器状态：
   1. 接口：public ScannerStatus getScannerStatus(int deviceId)
   2. 参数：扫描器ID
   3. 返回：

ScannerStatus: {

int deviceId; //扫描器ID

String name; //扫描器名称

int networkStatus; //网络状态：0-正常，1-异常

int interfaceStatus; //接口状态：0-正常，1-异常

ScannerServiceStatus serviceStatus; //服务状态

}

ScannerServiceStatus: {

int status; //状态：0-正常，1-异常

int numOfTasks; //任务数量

}

1. 任务控制接口（暂停、继续）
   1. 接口：public int ctrlScanningTask(String uuid, int opcode)
   2. 参数：uuid 任务识别ID；opcode 操作码：0-暂停，1-继续 ，2-终止
   3. 返回：0-成功，-1-失败

## 四．补充修订

1. 修改创建任务接口，回调通知变更为主动查询。

2． 查询详情的条件变更为任务识别码；识别ID由接口调用方提供，必须保证其唯一性。

3. 修改发送邮件接口参数类型；修改获取扫描器信息接口返回数据类型。

4. 修改获取任务状态接口，增加detailStatus字段，该字段为1时可调用getTaskScanDetail接口获取告警详情。

5. 修改获取扫描器信息接口，增加deviceType字段。

6. uuid生成方法：UUID.randomUUID().toString().replace(“-”, ””)

7. 修改获取扫描器信息接口，增加location字段。

8. 修改邮件通知接口，修改参数类型

9. 增加getHeartBeat接口

10. 增加getScannerStatus接口

11. 增加ctrlScanningTask接口

12. 邮件通知接口，增加收件人列表

13. 获取扫描器状态接口，增加参数和返回字段

14. 邮件通知接口，附件列表更改为单个附件

15. 任务控制接口，增加操作码2（停止任务）；暂停操作必须要在任务状态为扫描中时才能执行；继续操作必须要在任务状态为暂停时才能执行；WEB扫描任务只能停止无法暂停；该接口适合**执行时间比较久**的任务，因为状态更新有延迟可能会造成操作失败