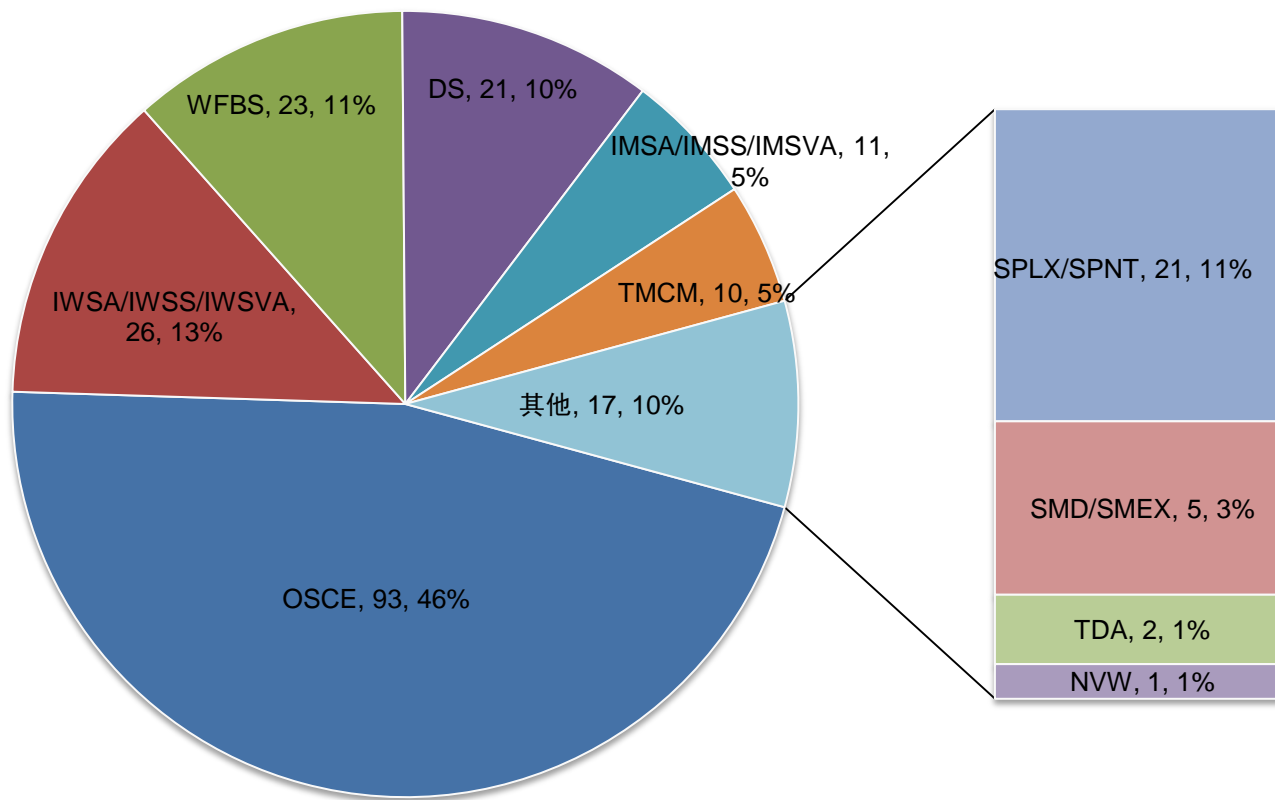


# 第二季趋势科技产品问题 总结与分享

Freda Zhang  
趋势科技培训部

# 第二季度产品案件排名



# 第二季度经典问题分享

# 案例一：OSCE案例

- 问题描述：
  - 用户的OSCE 8.0程序在打开控制台后提示无权限

# 案例一：OSCE案例

- 问题排错：
  - IIS日志

```
2013-06-03 10:16:51 W3SVC3 10.21.0.183 GET /officescan/console/html/cgi/cgiChkMasterPwd.exe - 4343 - 10.21.0.183 Mozilla/5.0+(Windows+NT+5.2;+rv:15.0)+Gecko/20100101+Firefox/15.0.1 403 19 1314
2013-06-03 10:17:03 W3SVC3 10.21.0.183 GET /officescan/console/html/cgi/cgiChkMasterPwd.exe - 4343 - 10.21.0.183 Mozilla/5.0+(Windows+NT+5.2;+rv:15.0)+Gecko/20100101+Firefox/15.0.1 403 19 1314
2013-06-03 10:17:03 W3SVC3 10.21.0.183 GET /officescan/console/html/cgi/cgiChkMasterPwd.exe - 4343 - 10.21.0.183 Mozilla/5.0+(Windows+NT+5.2;+rv:15.0)+Gecko/20100101+Firefox/15.0.1 403 19 1314
2013-06-03 10:17:04 W3SVC3 10.21.0.183 GET /officescan/console/html/cgi/cgiChkMasterPwd.exe - 4343 - 10.21.0.183 Mozilla/5.0+(Windows+NT+5.2;+rv:15.0)+Gecko/20100101+Firefox/15.0.1 403 19 1314
2013-06-03 10:17:07 W3SVC3 10.21.0.183 GET /officescan/console/html/cgi/cgiChkMasterPwd.exe - 4343 - 10.21.0.183 Mozilla/5.0+(Windows+NT+5.2;+rv:15.0)+Gecko/20100101+Firefox/15.0.1 403 19 1314
2013-06-03 10:17:08 W3SVC3 10.21.0.183 GET /officescan/console/html/cgi/cgiChkMasterPwd.exe - 4343 - 10.21.0.183 Mozilla/5.0+(Windows+NT+5.2;+rv:15.0)+Gecko/20100101+Firefox/15.0.1 403 19 1314
```

403.19 不能为这个应用程序池中的客户端执行 CGI

<http://support.microsoft.com/kb/318380/zh-cn>

# 案例一：OSCE案例

## • 解决方案：

1. 点击 [开始] > [所有程序] > [管理工具] > [Internet信息服务（IIS）管理器]

2. 展开OfficeScan所在服务器[服务器名（本地计算机）] > [应用程序池] > [DefaultAppPool], 检查[DefaultAppPool]是否处于运行状态。

右键点击选择“停止”，然后右键点击选择“启动”来重新启动 [DefaultAppPool], 检查问题是否能够解决。

3. 如果问题仍然存在，请右击[DefaultAppPool]，选择属性，点击[标识]选项卡，在“预定义帐户”中选择“本地系统”选项，点击[确定]，弹出确认窗口，点击[是]确认。

4. 重新启动IIS的服务，尝试打开控制台。

# 案例二：SPNT案例

- 问题描述：

- 在WINDOWS 2008 日上安装SPNT 5.8的时候提示“先前版本的SPNT驱动程序已经存在，请重新启动目标计算机并重试”
- 服务器上安装了OSCE的WEB控制台

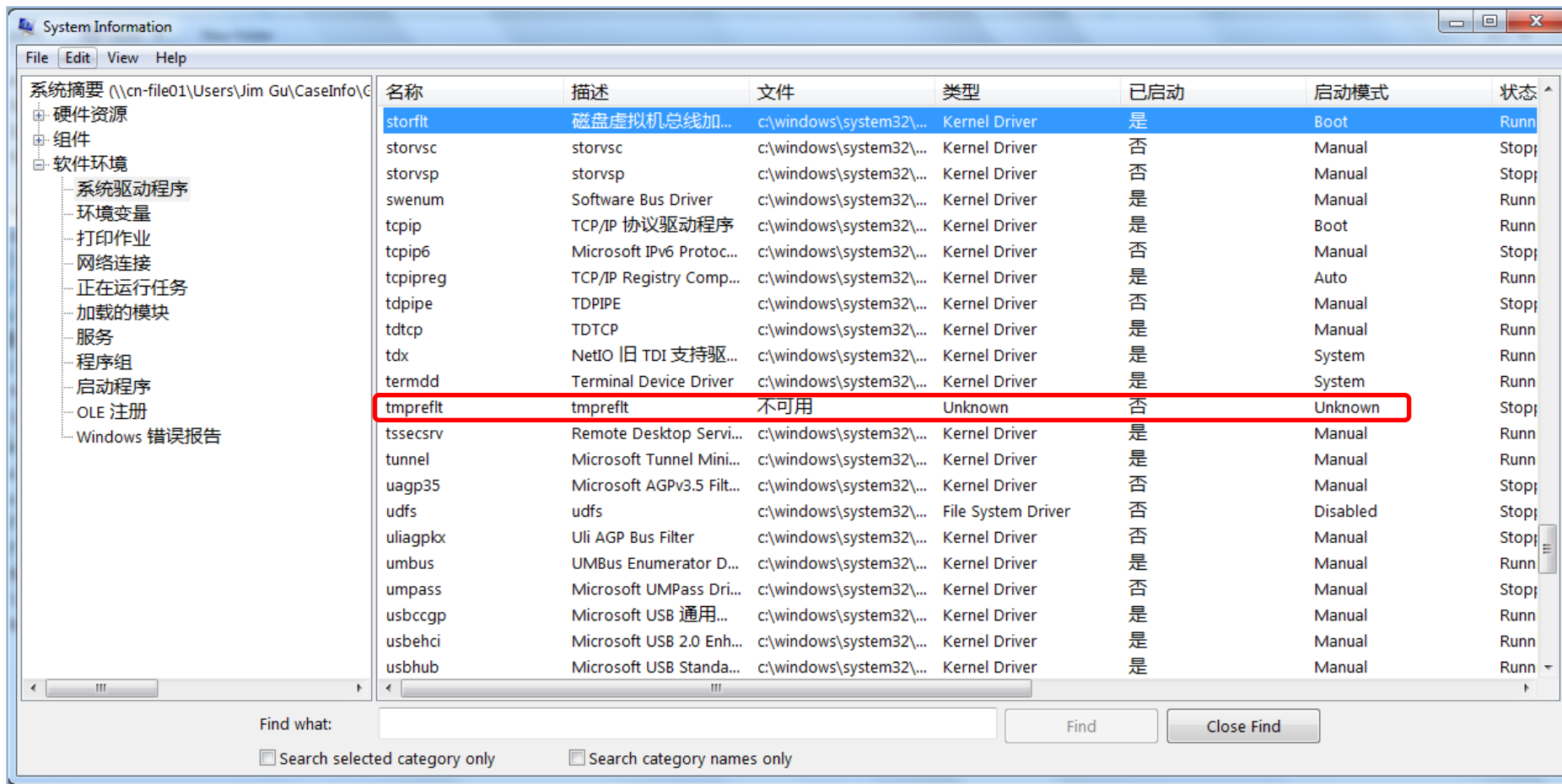


# 案例二：SPNT案例

- 问题排错：
  - 确认删除过SPNT在该机上的有关注册表键值（Solution 68451）
  - 电脑也重新启动过，仍不能成功安装
  - 收集安装日志sp5.log



# 案例二：SPNT案例



System Information window showing a list of drivers. The 'tmpprefit' driver is highlighted with a red box. The driver's status is 'Unknown' and it is marked as '不可用' (Unavailable).

名称	描述	文件	类型	已启动	启动模式	状态
storflt	磁盘虚拟机总线加...	c:\windows\system32\...	Kernel Driver	是	Boot	Runn
storvsc	storvsc	c:\windows\system32\...	Kernel Driver	否	Manual	Stopj
storvsp	storvsp	c:\windows\system32\...	Kernel Driver	否	Manual	Stopj
swenum	Software Bus Driver	c:\windows\system32\...	Kernel Driver	是	Manual	Runn
tcpip	TCP/IP 协议驱动程序	c:\windows\system32\...	Kernel Driver	是	Boot	Runn
tcpip6	Microsoft IPv6 Protoc...	c:\windows\system32\...	Kernel Driver	否	Manual	Stopj
tcpipreg	TCP/IP Registry Comp...	c:\windows\system32\...	Kernel Driver	是	Auto	Runn
tdpipe	TDPIPE	c:\windows\system32\...	Kernel Driver	否	Manual	Stopj
tdtcp	TDTCP	c:\windows\system32\...	Kernel Driver	是	Manual	Runn
tdx	NetIO 旧 TDI 支持驱...	c:\windows\system32\...	Kernel Driver	是	System	Runn
termdd	Terminal Device Driver	c:\windows\system32\...	Kernel Driver	是	System	Runn
tmpprefit	tmpprefit	不可用	Unknown	否	Unknown	Stopj
tssecsrv	Remote Desktop Servi...	c:\windows\system32\...	Kernel Driver	是	Manual	Runn
tunnel	Microsoft Tunnel Mini...	c:\windows\system32\...	Kernel Driver	是	Manual	Runn
uagp35	Microsoft AGPv3.5 Filt...	c:\windows\system32\...	Kernel Driver	否	Manual	Stopj
udfs	udfs	c:\windows\system32\...	File System Driver	否	Disabled	Stopj
uliagplx	Uli AGP Bus Filter	c:\windows\system32\...	Kernel Driver	否	Manual	Stopj
umbus	UMBus Enumerator D...	c:\windows\system32\...	Kernel Driver	是	Manual	Runn
umpass	Microsoft UMPass Dri...	c:\windows\system32\...	Kernel Driver	否	Manual	Stopj
usbccgp	Microsoft USB 通用...	c:\windows\system32\...	Kernel Driver	是	Manual	Runn
usbhci	Microsoft USB 2.0 Enh...	c:\windows\system32\...	Kernel Driver	是	Manual	Runn
usbhub	Microsoft USB Standa...	c:\windows\system32\...	Kernel Driver	是	Manual	Runn

# 案例二：SPNT案例

- 解决方案
  - 卸载tmpreflt驱动
  - 重启服务器
  - 重新安装SPNT

# 案例三：IMSS案例

- 问题描述：

The screenshot displays the Trend Micro InterScan Messaging Security Suite administration interface. The left sidebar contains a navigation menu with the following items: Summary, Policy, IP Filtering, Reports, Logs, Quarantine & Archive, Administration (highlighted with a red box), Updates, Notifications, IMSS Configuration, Connections, SMTP Routing (highlighted with a red box), Configuration Wizard, Admin Accounts, User Quarantine Access, Password, and Product License. The main content area is titled "SMTP Routing" and features four tabs: SMTP, Connections, Message Rule, and Domain-Based Delivery (highlighted with a red box). Below the tabs, the "Domain-Based Delivery" section includes "Add" and "Delete" buttons, a page indicator "1-2 of 2", and a "Page 1" dropdown. A table lists the domain-based delivery rules:

Domain	Delivery Method
<input type="checkbox"/> a.com	11.22.33.44:25
<input type="checkbox"/> sina.com	freemx1.sinamail.sina.com.cn:25

At the bottom of the table, there is a "15 per page" dropdown menu. Below the table are "Save" and "Cancel" buttons.

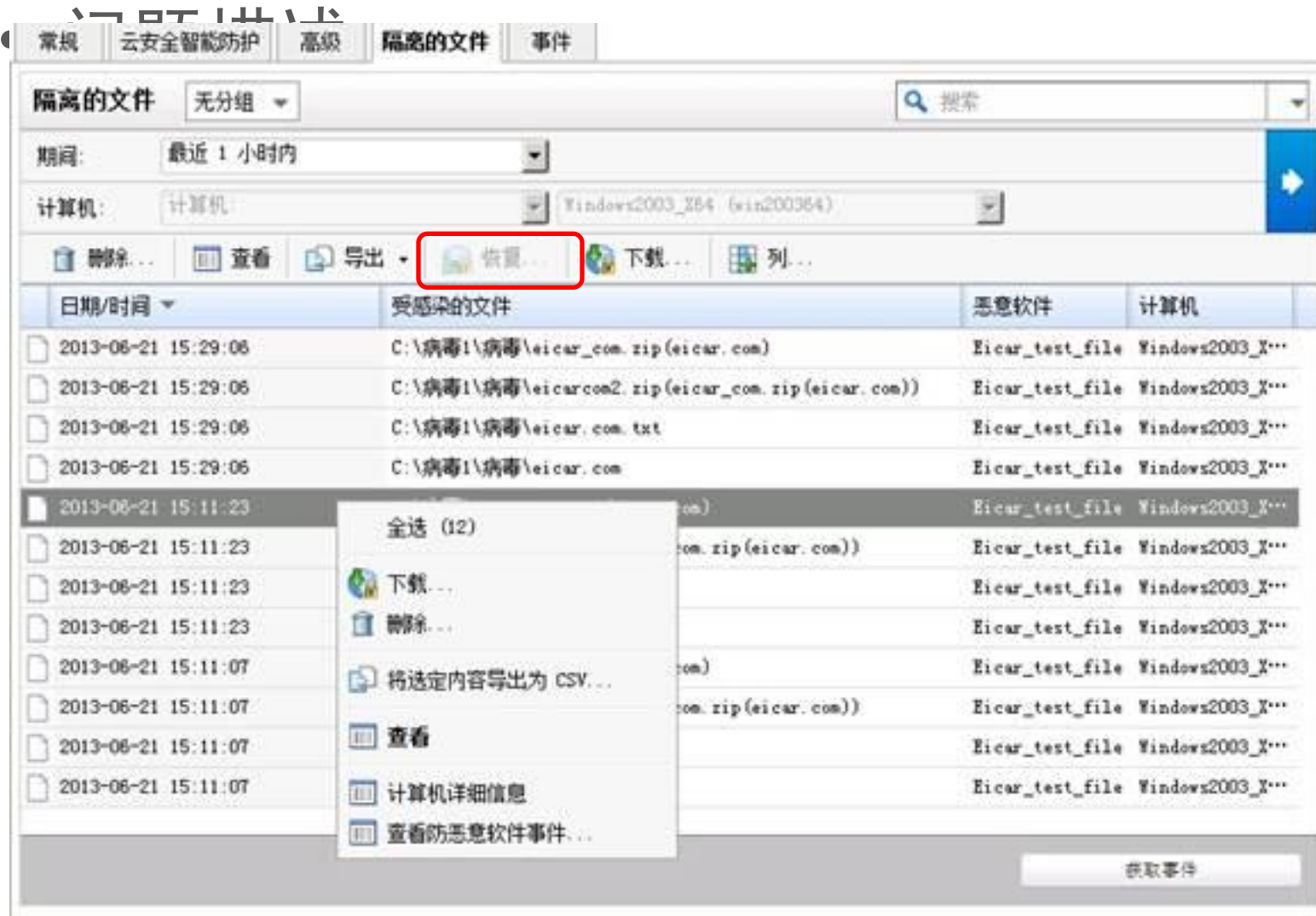
# 案例三：IMSS案例

- 问题分析：
  - IMSS在domain-based delivery里面无法将同样的域名添加两次
  - hand off操作基于某个action之后才会触发操
  - 无法满足客户的该需求

# 案例三：IMSS案例

- Workaround方法：
  - 在IMSA的domain-based delivery里面添加一条记录，邮件服务器的地址填写FQDN名而非IP地址
  - 通过客户的DNS或者在IMSS服务器的host文件中手动将该FQDN名指向多个IP来实现客户的需求

# 案例四：DS案例



恢复  
法通  
键



# 案例四：DS案例

日期/时间	受感染的文件	恶意软件	计算机
2013-06-21 16:24:29	C:\Documents and Settings\Administrator\Local Settings\Temp\eicar_...	Eicar_test_file	xp (XP)
2013-06-21 16:24:22	C:\Documents and Settings\Administrator\桌面\新建文件夹\eicar\eica...	Eicar_test_file	xp (XP)
2013-06-21 16:24:15	C:\Documents and Settings\Administrator\Local Settings\Temp\eicar_...	Eicar_test_file	xp (XP)
2013-06-21 16:24:09	C:\Documents and Settings\Administrator\Local Settings\Temp\eicar_...	Eicar_test_file	xp (XP)
2013-06-21 16:24:05	C:\Documents and Settings\Administrator\桌面\新建文件夹\eicar\eica...	Eicar_test_file	xp (XP)
2013-06-21 16:18:58	C:\Documents and Settings\Administrator\桌面\新建文件夹\eicar\eica...	Eicar_test_file	xp (XP)
2013-06-21 16:18:57	C:\Documents and Settings\Administrator\桌面\新建文件夹\eicar\eica...	Eicar_test_file	xp (XP)
2013-06-21 16:04:41	C:\Documents and Settings\Administrator\Local Settings\Temp\eicar_...	Eicar_test_file	xp (XP)
2013-06-21 16:04:38	C:\Documents and Settings\Administrator\Local Settings\Temp\eicar_...	Eicar_test_file	xp (XP)
2013-06-21 16:04:06	C:\Documents and Settings\Administrator\桌面\新建文件夹\eicar\eica...	Eicar_test_file	xp (XP)
2013-06-21 16:04:05	C:\Documents and Settings\Administrator\桌面\新建文件夹\eicar\eica...	Eicar_test_file	xp (XP)

DSA代理

- 下载... (📁) 可将隔离文件从计算机或虚拟设备移动到选定位置。
- 删除... (🗑️) 可从计算机或虚拟设备删除一个或多个隔离文件。
- 将有关隔离文件（并非文件本身）的信息导出 (📄) 为 CSV 文件。
- 查看隔离文件的详细信息 (📄)。
- 查看检测到恶意软件的计算机的计算机详细信息 (📄) 窗口。
- 查看防恶意软件事件... (📄) 显示与此隔离文件关联的防恶意软件事件。
- 添加或删除列 (📄) 通过单击添加/删除可添加或删除列。
- 搜索 (🔍) 特定隔离文件。

# 案例四：DS案例

- 结论：
  - 此“恢复”功能只适用于DSA,不适用与无代理防护



# 案例五：IWSA案例

- 问题描述：

- 用户部分手机端WIFI接入热点，无法通过QQ连接服务器
- 用户环境中问题了IWSVA5.1

# 案例五：IWSA案例

- 问题排错：
  - 其他桌面端及手机端的QQ都能正常访问服务器
  - 已检查其他防火墙或者可能做限制的设备，都已放行。

# 案例五：IWSA案例

- 问题分析：

- 当一些HTTP流量数据包格式不符合标准HTTPS流量的数据格式时会导致IWSVA无法正常处理这些流量

- 解决方法

- 通过开启tunnel\_non\_http\_traffic 功能避免IWSVA对这些流量造成影响

1. 使用SSH 方式登录IWSVA 5.1
2. 输入clish 命令进入IWSVA 命令行控制台
3. 输入 ‘enable’进入enable模式
4. 输入 ‘configure module http non\_http\_bypass enable’

# 哪些您可以自己解决？

问题名称	解决方案来源	备注
服务器安装/升级部署咨询	SOP、Readme、AG	包括咨询服务器如何安装/升级、服务器支持哪些哪些系统等。
客户端部署咨询	AG、Readme	包括咨询客户端有哪些安装方式、客户端如何安装、客户端支持哪些操作系统等。
服务器占用空间过大/OSCE 10.0 WSS文件夹过大	KB	
咨询OSCE是否有某些功能/某些功能如何设置	Readme、AG	
web控制台密码重置	KB	
恢复隔离文件	AG、KB	比如设备管理、漫游客户端等
咨询OSCE下载地址	官网下载专区	
客户端卸载/退出密码重置	下载专区	
需要文档	KB	包括管理员手册、安装部署手册
服务器更改IP/主机名/安装方式		
哪些版本OSCE能够注册TMCM	Readme	
如何设置服务器从其他更新源更新	KB、AG	

# 遇到问题怎么办？



## 简单处理

- 系统日志、报警信息等
- 重启计算机、进程、服务等

## 寻求帮助

- 产品知识库
- 自述手册、管理员文档等
- 趋势科技技术支持

## 深入判断

- 配置修改
- 参数调整
- 调试日志分析等

# 产品基本信息获取

产品主页—关于

趋势科技产品名

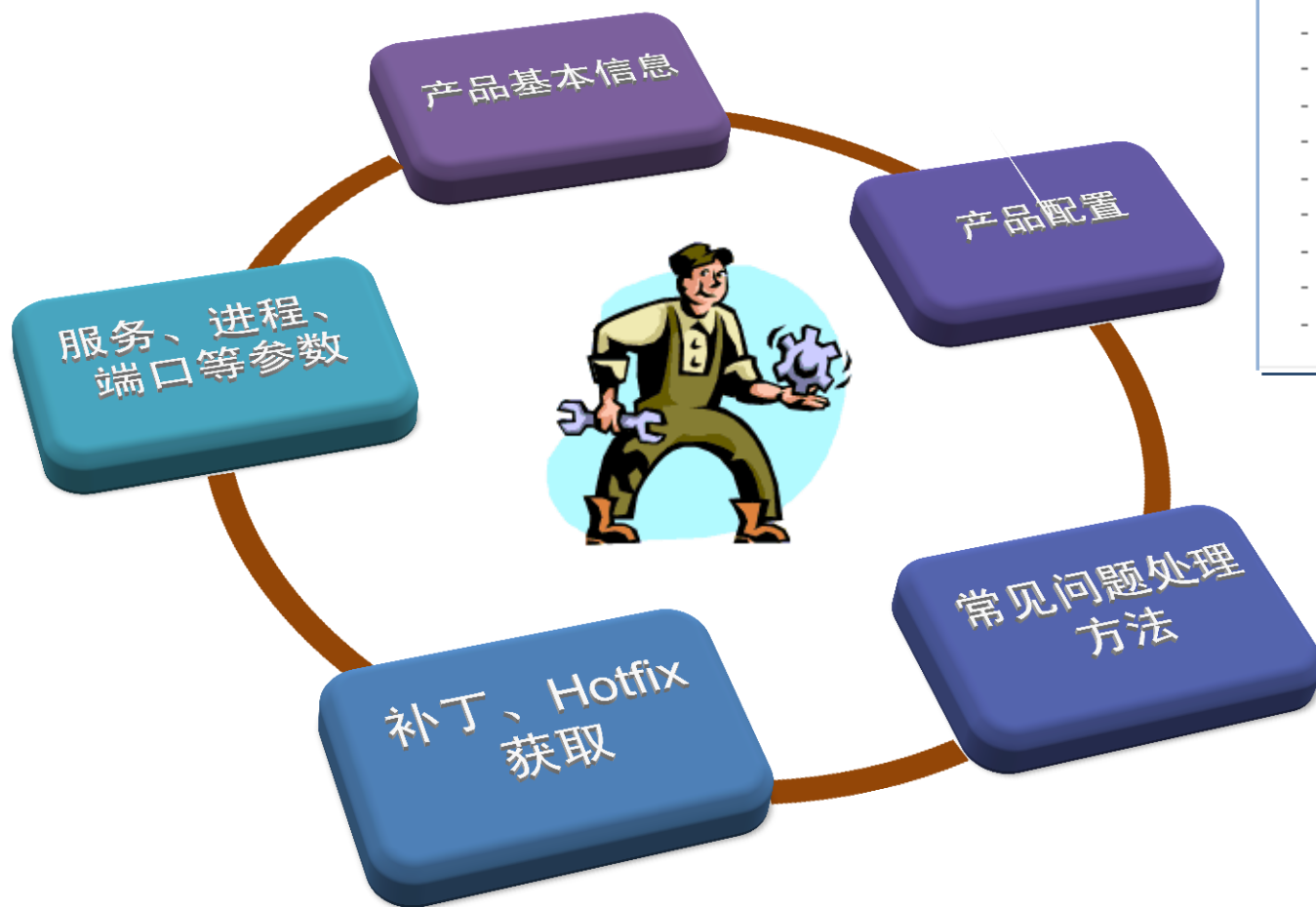
产品版本

Build号

语言版本

了解产品基本信息，有助于问题有效解决

# 产品知识库中有些什么？



## 技术支持

- 咨询百科
- 常见问题及解答
- 下载专区
- 相关公告
- Beta产品测试
- 产品试用评估
- 新病毒码文件格式
- TCSE 专区
- 在线注册
- 在线提交问题
- BBS病毒版块
- TCAE交流专区
- 技术支持

# 知识库之搜索

- 选择正确参数帮助你获取最佳结果

**技术支持** 需要访问最新, 最详细的信息?  
请至[全球咨询百科站点\(英文\)](#)

---

请选择要查看的解决方案:

---

热点解决方案

- > [有关预防和处理ARP攻击病毒的说明 \(HOT\)](#)
- > [有关趋势科技发布新病毒特征码加入的Flag/No Action/GenMajorType处理措施的FAQ说明 \(HOT\)](#)
- > [升级最新的SPS后可能会引起部分IMSS for NT 5.5服务运行不稳定 \(HOT\)](#)
- > [升级InterScan Messaging Security Suite\(IMSS\) 5.5 for Windows\(Builds 1107-1186\)至Service Pa... \(HOT\)](#)
- > [安装趋势科技PC-cillin云安全软件2012全功能增强版检查系统需求时, 提示安装停止。](#)

---

搜索咨询百科

产品名称:

类别:

关键词:

版本:

最多返回结果:

解决方案编号:



# 知识库之关键字

- 问题类别
  - 更新、配置、升级、安装等
- 错误提示
  - “错误的应用程序 Dbserver.exe”
- 日志结果
  - 日志文件名
  - 日志中错误信息等

*Faulting application DbServer.exe, version 10.0.0.1895, time stamp 0x4b6bdb4e, faulting module DbServer.exe, version 10.0.0.1895, time stamp 0x4b6bdb4e, exception code 0x40000015, fault offset 0x000c91b0, process id 0x1dfc, application start time 0x01cafb39285abdb6.*

# 常用文档资料获取

管理员手册

SOP文档

升级文档

自述文件

.....

The screenshot shows a web browser window with the URL <http://support.trendmicro.com.cn/TM-Product/Document/SOP/>. The page title is "support.trendmicro.com.cn - /TM-P". The main content area displays a list of links and dates, organized into a table-like structure. The links are underlined and colored blue, while the dates are in black. The table includes a link for "[To Parent Directory]" and a list of links with corresponding dates and times.

Link	Date	Time	Link
<a href="#">[To Parent Directory]</a>			
<a href="#">DLP</a>	2011年1月6日	17:38	<dir> <a href="#">DLP</a>
<a href="#">DS</a>	2012年7月16日	17:11	<dir> <a href="#">DS</a>
<a href="#">IGSA</a>	2010年7月30日	15:11	<dir> <a href="#">IGSA</a>
<a href="#">IMSA</a>	2010年7月30日	15:12	<dir> <a href="#">IMSA</a>
<a href="#">IMSS</a>	2010年9月20日	15:05	<dir> <a href="#">IMSS</a>
<a href="#">ISVW</a>	2010年7月30日	15:26	<dir> <a href="#">ISVW</a>
<a href="#">ISWP</a>	2010年7月30日	15:26	<dir> <a href="#">ISWP</a>
<a href="#">IWSA</a>	2011年6月24日	10:20	<dir> <a href="#">IWSA</a>
<a href="#">IWSS</a>	2010年7月30日	15:28	<dir> <a href="#">IWSS</a>
<a href="#">NVWE</a>	2010年9月10日	17:12	<dir> <a href="#">NVWE</a>
<a href="#">OSCE</a>	2011年11月3日	15:50	<dir> <a href="#">OSCE</a>
<a href="#">SMD</a>	2010年7月30日	15:33	<dir> <a href="#">SMD</a>
<a href="#">SMEX</a>	2010年11月22日	15:12	<dir> <a href="#">SMEX</a>
<a href="#">SPLX</a>	2010年7月30日	15:40	<dir> <a href="#">SPLX</a>
<a href="#">SPNT</a>	2011年2月23日	17:57	<dir> <a href="#">SPNT</a>
<a href="#">TMCM</a>	2010年11月11日	16:32	<dir> <a href="#">TMCM</a>
<a href="#">TMMS</a>	2010年7月30日	15:45	<dir> <a href="#">TMMS</a>
<a href="#">WFBS</a>	2012年1月12日	16:24	<dir> <a href="#">WFBS</a>



TREND  
MICRO™  
趋势科技

[ 全程护航  
迈向云端 ]

# 谢谢!

爱趋势互动社区 [www.iqushi.com](http://www.iqushi.com)



[趋势CEO Eva微博](#)



[趋势官方微博](#)



[趋势云计算安全博客](#)



[趋势云计算安全网站](#)