TREND MICRO 趋势科技

全程护航
迈向云端

# 2012 Q2 售后常见问题与解决思路

# 2012 Q2 售后问题总结

- 售后问题最多的产品TOP 3
  - OfficeScan
  - InterScan Web Security Suite
  - Deep Security

# OfficeScan问题分类

| OfficeScan | 97 |
|---|---|
| 3rd Party Software Compatibility | 3 |
| Component Deployment from Server | 2 |
| Network | 1 |
| Network Slow-down | 1 |
| Process (Exception) | 2 |
| Product Configuration | 45 |
| System Crash / Halt (Blue Screen) | 4 |
| System Slow-down | 7 |
| Trend Product Performance | 3 |
| UI Functional Defect / Errors | 21 |
| UI Grammar / Typo | 2 |
| Update from Internet (ActiveUpdate) | 2 |
| Update from Second-Tier Products Update source | 3 |
| Update Process Issues | 1 |

# InterScan Web Security Suite问题分类

| InterScan Web Security Suite | 39 |
|---|---|
| 3rd Party Software Compatibility | 1 |
| Hardware Failure | 4 |
| License certificate or AC Lookup | 1 |
| Network | 1 |
| Network Slow-down | 1 |
| Product Configuration | 15 |
| System Crash / Halt (Blue Screen) | 2 |
| Trend Product Performance | 2 |
| UI Functional Defect / Errors | 6 |
| Update from Internet (ActiveUpdate) | 2 |
| Update Process Issues | 1 |
| (blank) | 3 |

# Deep Security问题分类

| Deep Security | 37 |
|---|---|
| 3rd Party Application | 3 |
| 3rd Party Software Compatibility | 2 |
| Generic Detection | 1 |
| Network | 1 |
| Process (Exception) | 1 |
| Product Configuration | 19 |
| Product Features | 1 |
| System Crash / Halt (Blue Screen) | 1 |
| System Slow-down | 2 |
| Trend Product Compatibility | 1 |
| UI Functional Defect / Errors | 4 |
| Update from Internet (ActiveUpdate) | 1 |

# OfficeScan摘要页面异常（一）

- 现象
  - 登录管理控制台，提示Unable to display data beacause of an unexptected error. Please try again later.
- 可能原因
  - C:\windows\temp\文件夹的IUSER账号没有足够权限
- 处理方法
  - 在OfficeScan服务器上，打开C:\WINDOWS\Temp\目录的安全属性
  - 添加以下账户名称
    IUSR_servername
    Network Service
  - 给予账户读和写权限
  - 重启OfficeScan服务

# OfficeScan摘要页面异常（二）

- 现象
  - 打开控制台后反复提示需要下载index.php文件
- 可能原因
  - 误删除了OSCE服务器上的php程序
- 处理方法
  - 在OSCE 服务器端下载并保存 php-5.3.5-nts-Win32-VC9-x86.msi，http://windows.php.net/downloads/releases/archives/php-5.3.5-nts-Win32-VC9-x86.msi
  - 以管理员身份运行命令提示符
  - 将路径转换到之前PHP程序所在的路径
  - 运行以下命令:
    msiexec /i php-5.3.5-nts-Win32-VC9-x86.msi /q ADDLOCAL=iis4FastCGI,ext_php_gmp,ext_php_openssl,ext_php_pdo_sqlite,ext_php_ldap,ext_php_curl /L C:\PHPInstall.log

# OfficeScan 客户端与服务器端的连接问题

- 问题原因
  - OfficeScan客户端发生以下状况会通知服务端:
    - 退出OfficeScan客户端 (右键点击OfficeScan图标,然后选择退出)。
    - 通过添加/删除程序或使用的OfficeScan卸载程序来卸载OfficeScan客户端。
    - 通过系统服务控制台,停止OfficeScan client services。
    - 移动OfficeScan客户端从一台服务器到另一台服务器。
  - OfficeScan客户端发生以下状况不会通知服务端
    - 从网络断开,拔掉网线或者网卡被禁用。
    - 用任务管理器或其他第三方进程管理工具,结束或终止客户端进程。
    - 手动移动或删除OfficeScan客户端的组件或者注册表信息。
    - 利用卸载工具,脱掉,删除OfficeScan安装客户端组件,文件和目录。
    - 没有适当的写在OfficeScan客户端,就格式化磁盘或者恢复磁盘镜像。
- 解决思路
  - 设置预设验证
  - 设置事件触发更新

# IWSVA 部署后出现网络故障

- 如何查看网络连接情况
  - 查看CPU和内存利用率：atop
  - 查看TCP 80建立的连接数量：netstat -na|grep ESTABLISHED|grep ":80 "|wc –l
    - 当工作在桥接模式下，结果除以2
  - 查看建立连接最多的IP地址：netstat -na|grep ESTABLISHED|awk '{print$5}'|awk -F: '{print$1}'|sort |uniq -c| sort –r
  - 查看发起连接最多的IP地址：netstat -na|grep SYN|awk '{print$5}'|awk -F: '{print$1}'|sort |uniq -c| sort –r
- 日志收集
  - 网络抓包（不要超过3分钟）
    - tcpdump -i eth1 -s 0 -w \etc\iscan\UserDumps\eth1.pcap&
    - tcpdump -i eth2 -s 0 -w \etc\iscan\UserDumps\eth2.pcap&
    - tcpdump -i br0 -s 0 -w \etc\iscan\UserDumps\br0.pcap&
  - 打包系统性能日志：/var/monitor/collect_monitor.sh
  - IWSA 系统信息日志：IWSA 管理控制台-管理-支持页面-“生成系统信息文件”

# 部署Deep Security 产品时ESXi是否需要重启

- 在部署DS时，以下情况需要重启ESXi主机
  - 在对ESXi 执行准备（prepare）操作时需要重启ESXi服务器
  - 安装ESXi 补丁时需要重新启动
  - 调整ESXi heap memory设置（针对DSVA 的性能调整）

TREND MICRO 趋势科技

全程护航
迈向云端

# Thanks !

爱趋势互动社区 www.iqushi.com

CEO Eva微博　趋势云安全博客　趋势官方微博