某局点部分终端防病毒软件检查不通过

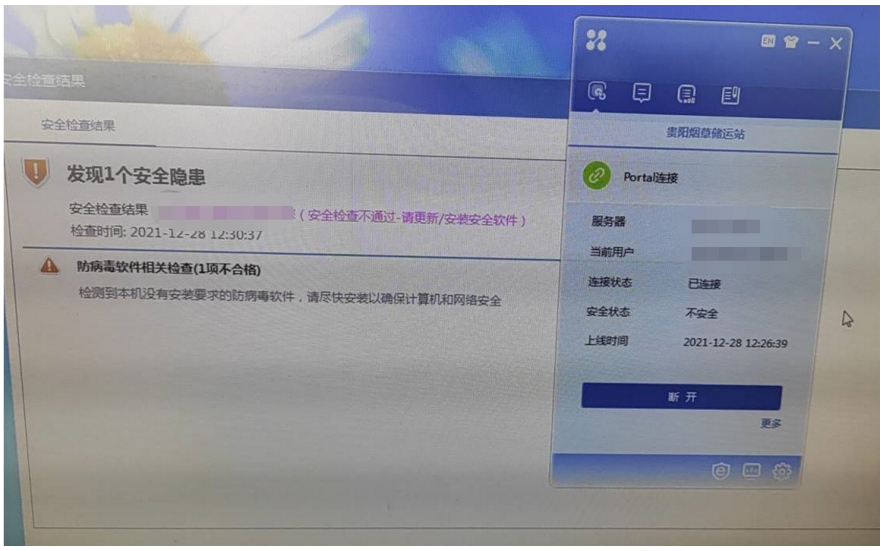
PLAT iMC 高洋 2021-12-31 发表

组网及说明

不涉及

问题描述

某局点用iNode进行portal认证并进行防病毒软件检查，使用相同的安全策略和软件版本，部分终端可以检查通过，部分不可以，不可以的终端windows7和windows10都有。



过程分析

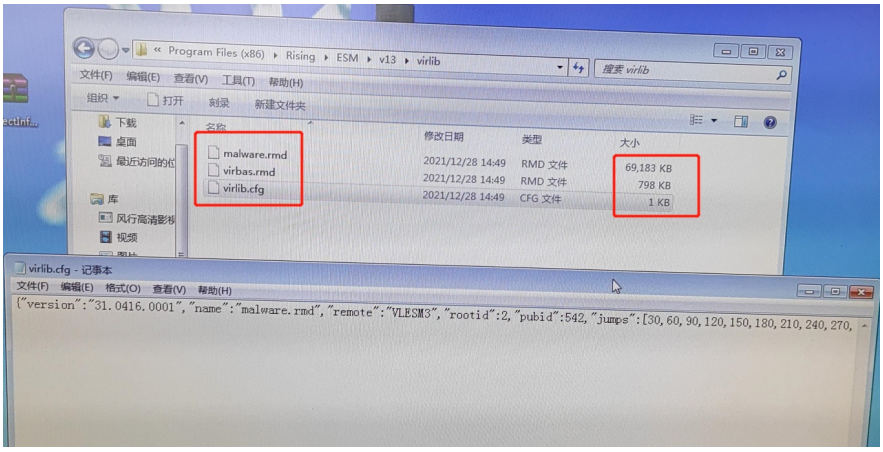
（1）识别不了的终端是否都是64位操作系统或者32位操作系统，怀疑是操作系统的问题；

现场不能识别防病毒软件的终端均为32位，但是有其他32位终端可以被识别，排除操作系统问题；

（2）收集inode详细级别日志和policyserver日志，日志提示未检查到终端安装的防病毒软件；

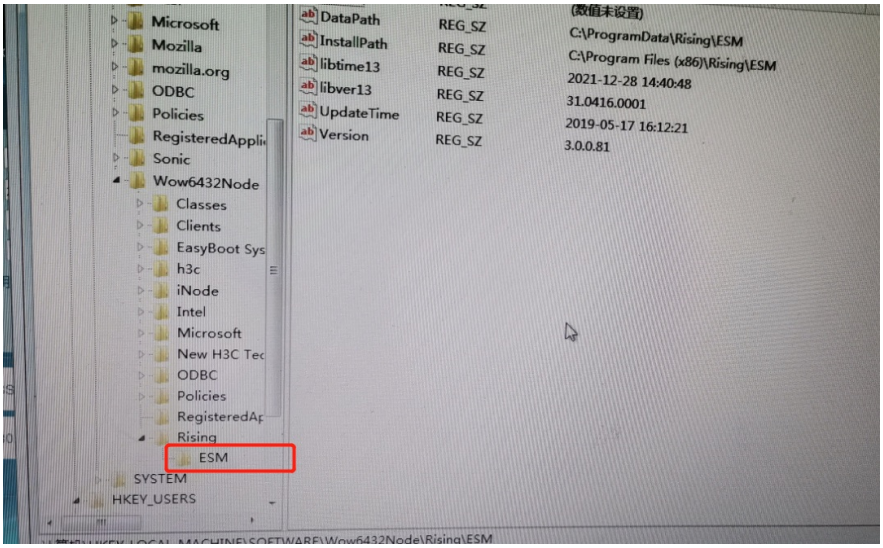
```
[2021-12-28 12:29:19] [Dbg] [1440] SecPkt secDataProc: The type is 6
[2021-12-28 12:29:19] [Dbg] [1440] SecPkt secDataProc: The id is 14240
[2021-12-28 12:29:19] [DtlCmn] [1440] SecPkt sndSecMsg: transfer [6] [14240]
<data>
  <i n="action">repair</i>
  <i n="patchFailStamp">2NDOXkXvVt8=</i>
  <i
n="netScanPolicy">samplingInterval=30;IPPktPeak1=1000;IPPktPeak2=1100;NUcastPktsPeak1=10000;NUcastPktsPeak2=10100;PktsPeak1=100;PktsPeak2=110;IPC
onnPeak1=10000;IPConnPeak2=10100</i>
  <i n="netMonItem">IPPkt;NUcastPkt;Pkts;IPConn</i>
  <i n="avFailMessage">贵阳烟叶储运站-提示您（安全检查不通过-请更新/安装安全软件）</i>
  <i n="dissatisfactory">AV-Software|repair</i>
  <i n="virusUpdateUrl"/>
  <i n="virusUpdateUrlForIPv6"/>
  <i n="repairPolicy">Virus-Manual-Update</i>
  <i n="checkFailMessage">贵阳烟叶储运站-提示您（安全检查不通过-请更新/安装安全软件）</i>
  <i n="checkFailThresholdMessage"/>
  <i n="repairUrlStr">请点击此链接进行修改</i>
```

（3）怀疑是inode没有识别出安装的防病毒软件，检查以下文件夹中的文件数量和大小；

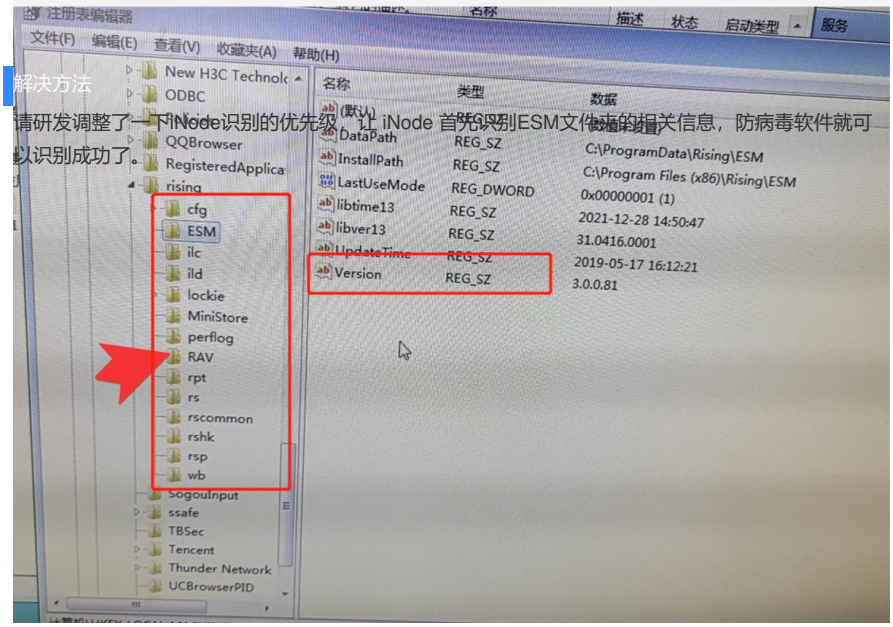


（4）打开注册表编辑器，查看该路径下的注册表信息；

正常应该为：rising下只有一个ESM；



现场环境：



解决方法

请研发调整了一下iNode识别的优先级，让 iNode 首先识别ESM文件夹的相关信息，防病毒软件就可以识别成功了。

主要问题来自于终端，该终端可能之前安装过一些瑞星防病毒软件，之后没有卸载干净，注册表多了很多干扰文件夹，正常安装就只有一个esm。现场环境还有许多文件夹，查看RAV文件，也有相关“version”信息，会给inode造成干扰，导致识别不出；