1. Reporter 组件网关系统存在命令执行漏洞修复报告

漏洞名称	Reporter 组件网关系统存在命令执行漏洞
影响范围	固件版本为 2021 年 8 月份之前的视频防火墙、网络安全审计系统（SURF-SA-RAG、SURF-RAG）、视频防泄密网关
排查方式	**网络安全审计系统：** 使用 admin 账号登录，点击 web 页面上的“详细”  查看系统当前版本的 build 号，如果 build 号为 21 年 8 月份之前，则需要进行系统版本升级。 **视频防火墙/视频防泄密网关：** 使用 admin 账号登录，查看页面又上角的系统版本信息，确定当前版本的 build 号  ，如果是 21 年 8 月份之前的版本，则需要进行系统版本升级。
漏洞产生原因分析	**产生原因：**自身开发原因 **具体原因：** **研发：** 1.系统程序中 PHP 代码使用 ROOT 权限执行，且没有对输入参数中包含的如’ `|等管道符进行参数校验，没有过滤或者转义这些字符，导致执行脚本漏洞的风险。并在页面 toQuery.php 产生脚本执行漏洞 2.页面权限控制问题，有些页面没有控制做鉴权后才能访问 3.系统使用的 Lighttpd WEB 服务器版本较低，未对一些 WEB

风险访问行为做控制

代码分析：

漏洞形成原因的代码分析 触发位置： /view/Behavior/toQuery.php 代码如下：

```
<?php
session_start ();
if ($_GET ["objClass"] == "")
  exit ();
$param = $_REQUEST;

//echo "\n--------------------------\n";
//print_r($param);
//echo "\n--------------------------\n";
if ($_GET ["method"] == "getList" || $_GET ["method"] == "import")
{
 $param ["user"] = $_SESSION ["s_userName"];
  $param ["lan"] = $_SESSION ["lan"];
  $param ["s_userPath"] = $_SESSION ["s_userPath"];
  exec ( "rm -rf /tmp/cache" );
  $cmd = "/usr/local/php/bin/php
/var/www/reporter/system/behavior/behavior_query.php";
  $cmd .= " " . $_GET ["objClass"];
  $cmd .= " " . $_GET ["method"];
  $cmd .= " " . base64_encode ( json_encode ( $param ) );
  exec ( $cmd . " > /dev/null &" );
} else {
  require_once ($_SERVER ["DOCUMENT_ROOT"] .
"/system/behavior/behavior_Detail.php");
  $obj = new QueryInterface ();
  $instance = $obj->getInstance ();
  $instance->invokeMethod ( $_GET ["objClass"], $_GET ["method"],
$param );
}
exit ();
?>
```

首先该页面未鉴权，允许前台直接访问。我们发现有 exec 这个函数，函数

	中包含变量$cmd， 查看$cmd 变量的来源，寻找我们可控的点。 可以发现$*GET["objClass"]和$*GET["method"]可控，根据执行条件， $*GET["method"] 需要等于 getList 或者 import 。而*$GET["objClass"]直接带入命令执行，只需要%0a 绕过即可。 **测试：**测试不全面
修复方案	**研发：**在 PHP 代码中对管道符进行转义或者过滤，页面编码进行规范。 对页面权限进行控制，非必要的页面都需要经过鉴权后才能访问 更新WEB 服务器Lighttpd的版本,新的版本中对该漏洞进行了修复。 **测试：**对发布版本进行验证后发布版本。
用户处置漏洞方式	升级系统版本
厂商补丁链接	**网络安全审计系统 32 位操作系统漏洞修复完成固件下载链接：** 链接：https://pan.baidu.com/s/1mjIZKEeY-XCQn3XUA6MP8A 提取码：799g MD5：df9c1dca3fa03ca5a777c318ef44bbcf **网络安全审计系统 64 位操作系统漏洞修复完成固件下载链接：** 链接：https://pan.baidu.com/s/1RcC-0wrSazncaAL3-S5HCw 提取码：t63m MD5：c651322f169da3f9c180c4ae4f61c7bd **视频防火墙修复完漏洞固件下载链接：** 链接：https://pan.baidu.com/s/1Db0oM5FLmU7-de-FbSaavw 提取码：ced6 MD5：fc5334b926287b69692e7bf0b05e611e **视频防泄密网关修复完漏洞后固件下载链接：** 链接：https://pan.baidu.com/s/1Mrmt9y0GYwD0zo_gUxSU4g

	提取码：4gfj　　MD5：071de8d8d90cd433c0e20b20e538ee34
相关附件	请见附件内容--系统升级指导文档V3.0。