通达OA绕过身份验证+任意文件上传RCE

原创 li9hu Timeline Sec
2020-08-27原文

收录于话题
#漏洞复现 111
#通达OA 3
#漏洞复现文章合集 70

上方蓝色字体关注我们，一起学安全！

本文作者：li9hu@Timeline Sec

本文字数：1024

阅读时长：3~4min

声明：请勿用作违法用途，否则后果自负

0x01 简介

通达OA采用基于WEB的企业计算，主HTTP服务器采用了世界上最先进的Apache服务器，性能稳定可靠。数据存取集中控制，避免了数据泄漏的可能。提供数据备份工具，保护系统数据安全。多级的权限控制，完善的密码验证与登录验证机制更加强了系统安全性。

0x02 漏洞概述

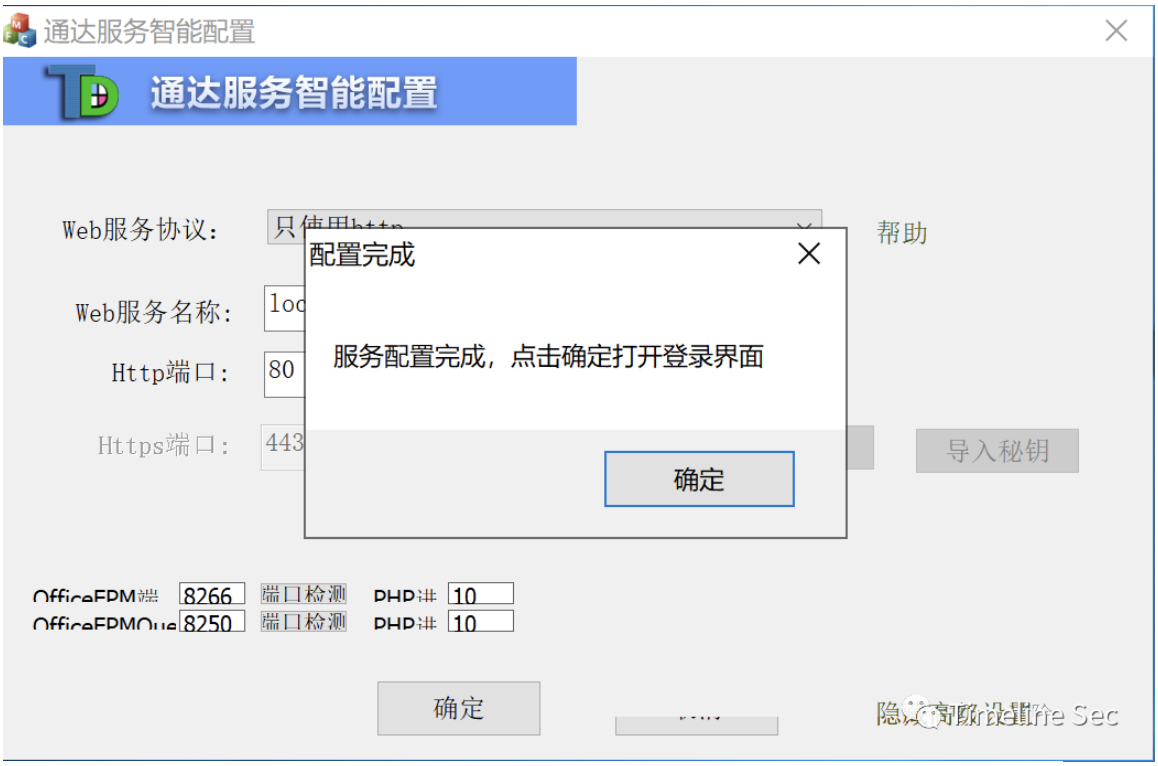
该漏洞是由于通过删除通达OA身份认证文件达到绕过登录限制，结合任意文件上传达到RCE的效果。

0x03 影响版本

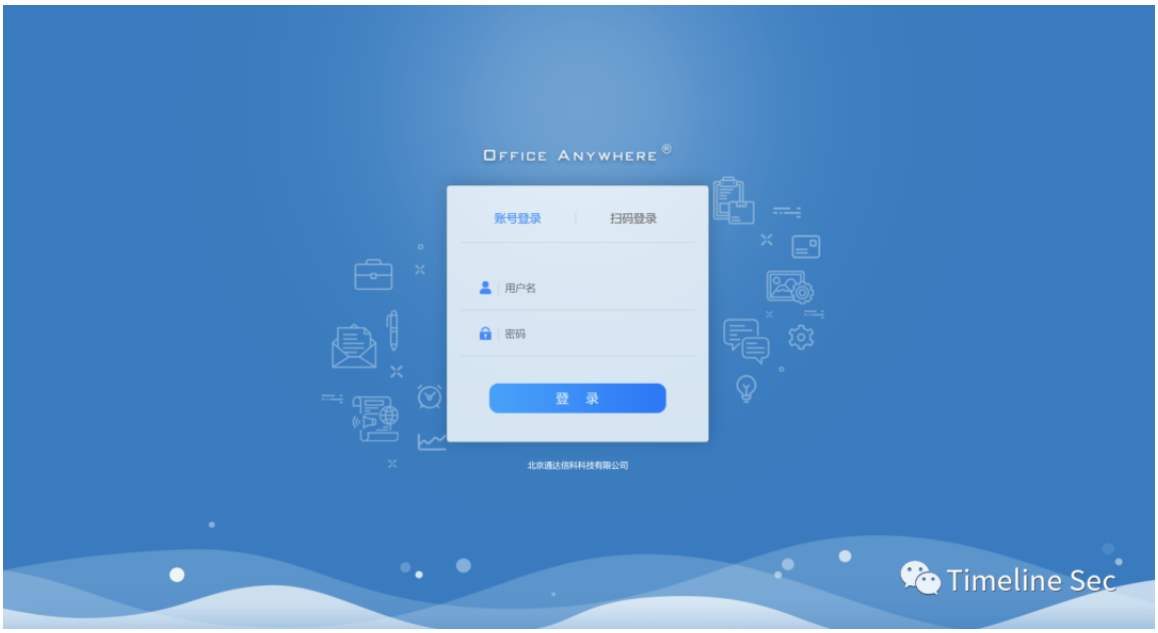
通达OA<v11.5&v11.6版本

0x04 环境搭建

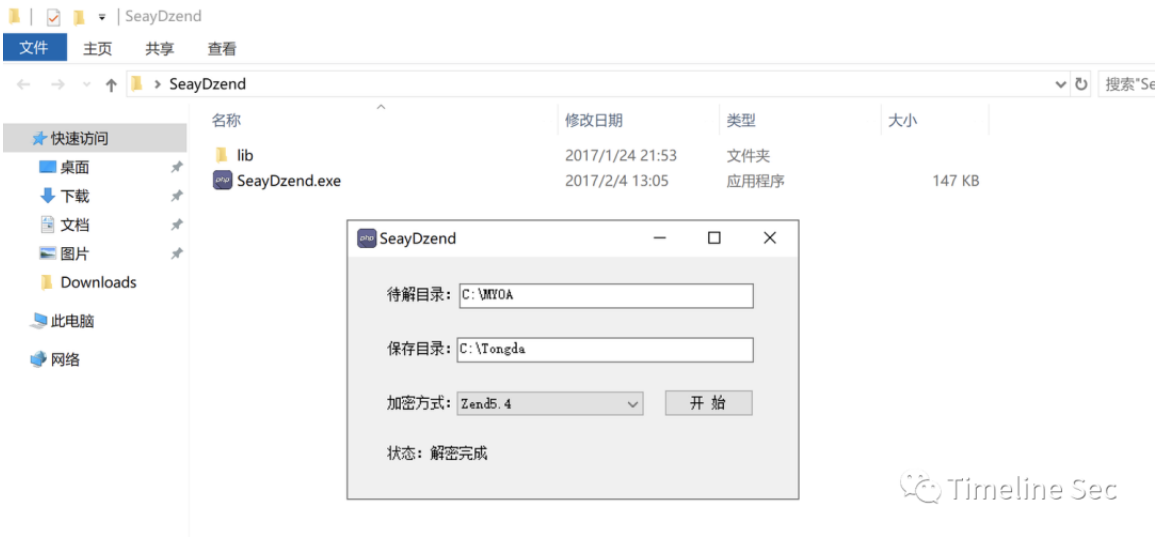
公众号内回复"通达OA11.6"获取安装包
在 Windows 下 直 接 双 击 安 装



点击确定访问



OA管理员用户名：admin 密码为空
使用解密工具SeayDzend解密源码



0x05 漏洞复现

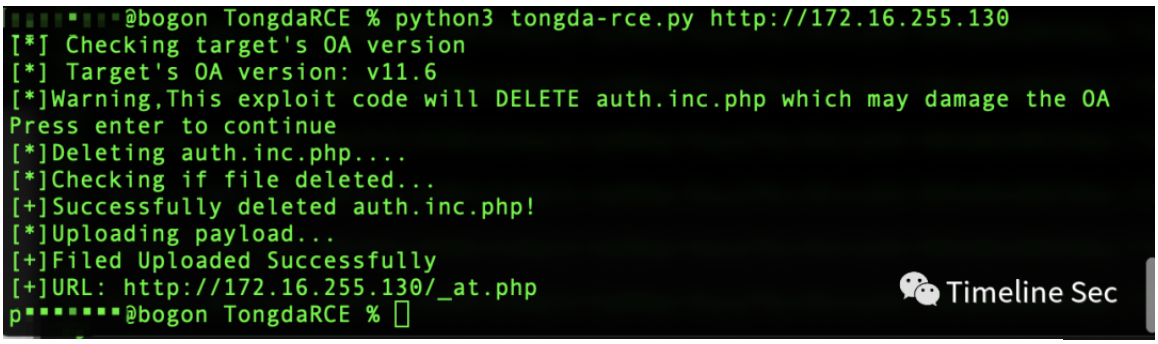
注意！该漏洞会删除服务器上的文件！谨慎复现！

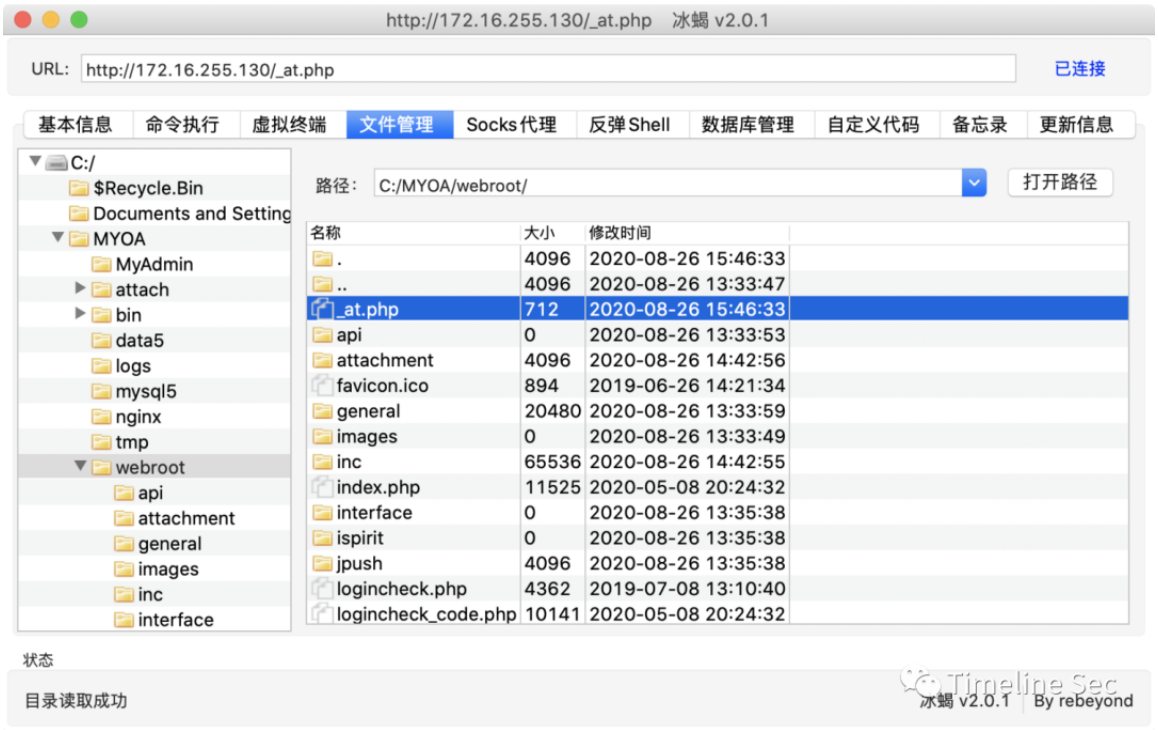
工具下载地址：

https://github.com/admintony/TongdaRCE

使用脚本删除文件后再登陆会变成这样

所以，请勿使用在线环境进行复现，请自行搭建！





0x06 漏洞分析

从网上公布的EXP可以知道会删除掉auth.inc.php文件，该文件是通达用于做身份验证的，需要登录访问的文件都会将它包含进来.包括后面需要用到的upload.php也包含了此文件，但是是通过include包含进来的区别于require若包含文件不存在include是不会导致程序终止的。

接着定位到任意文件删除的漏洞点/module/appbuilder/assets/print.php。直直白白，打头6行代码就实现了任意文件删除。

只要GET传值guid=../../../webroot/inc/auth.inc.php,带入unlink就可以删除上面介绍的身份验证文件，那么大多数需要身份验证的地方将失效。

print.php

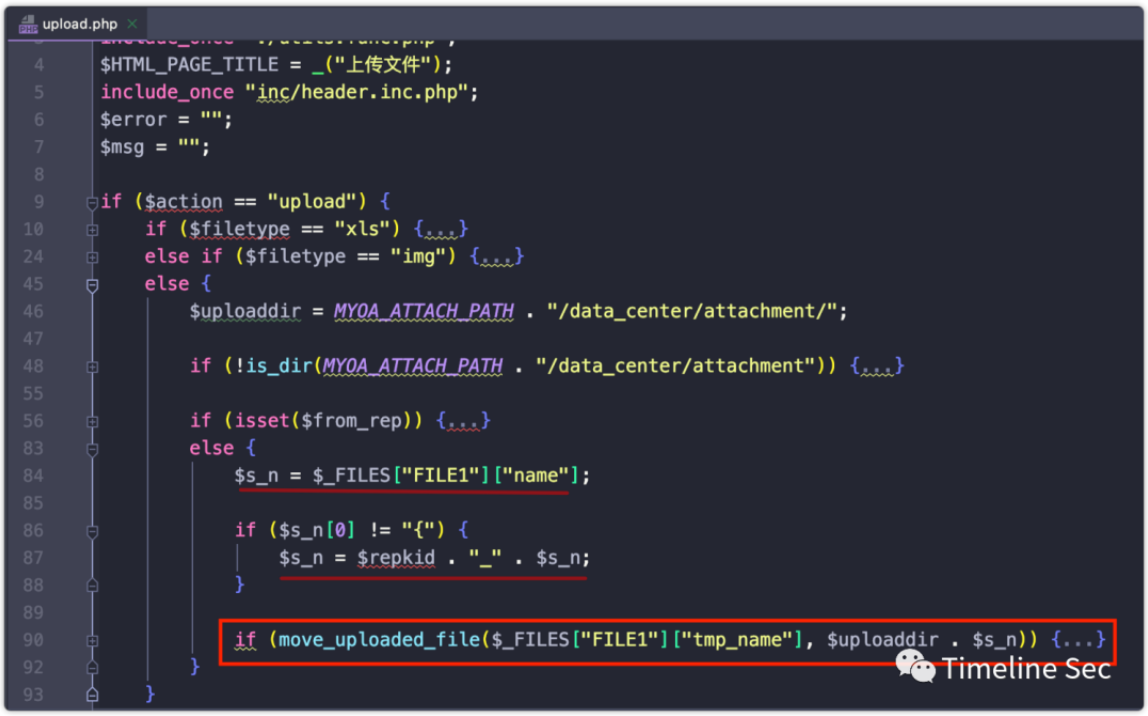
```php
<?php
$s_tmp = __DIR__ . "/../../../../logs/appbuilder/logs";
$s_tmp .= "/" . $_GET["guid"];
if (file_exists($s_tmp)) {
    $arr_data = unserialize(file_get_contents($s_tmp));
    unlink($s_tmp);
```


再介绍upload.php利用之前，先讲一下通达OA祖传变量覆盖。这里有个坑就是，有的解密工具会漏掉一个$，导致掉了一键盘的头发也不明白变量覆盖在哪里...因为该文件是common.inc.php，可想而知大部分文件都有包含，大部分地方可以拿变量覆盖来激情操作。

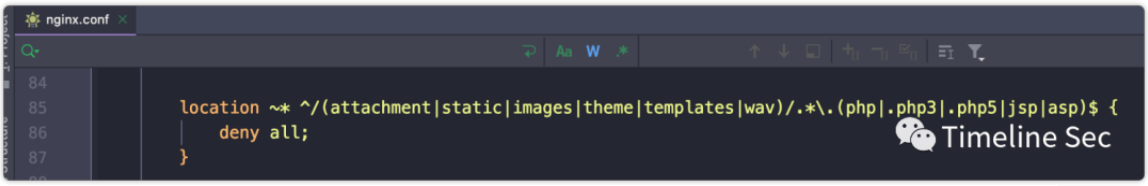
common.inc.php

```php
if (0 < count($_COOKIE)) {...}
if (0 < count($_POST)) {...}
if (0 < count($_GET)) {
    foreach ($_GET as $s_key => $s_value ) {
        if (substr($s_key, 0, 7) == "_SERVER") {
            continue;
        }

        if (!is_array($s_value)) {
            $_GET[$s_key] = addslashes(strip_tags($s_value));
        }

        ${$s_key} = $_GET[$s_key];
    }

    reset($_GET);
}

unset($s_key);
unset($s_value);
```

接着定位到上传点/general/data_center/utils/upload.php，第9行变量覆盖action为upload盘进if，接着我们upload位置就是/data_center/attachment了。第84行变量覆盖s_n为我们的恶意文件，90行upload位置拼接上s_n就是我们最终文件所在的位置。这里在87行变量覆盖repkid为../../../就能目录穿越将我们的马儿放在其他目录下，至于为什么后面会说。



参考了前辈文章，之所以要目录穿越到其他位置存放马，是因为通达OA的nginx限制了attachment目录下文件访问的权限，导致我们无法正常解析我们的马。~* 表示正则模式，匹配到以attachment开头的任意php等敏感文件都不允许。



0x07 修复方式

更新至官方最新版本。

参考链接：

https://drivertom.blogspot.com/2020/08/oa116-preauth-rce-0day.html

阅读原文看更多复现文章

Timeline Sec 团队

安全路上，与你并肩前行

精选留言

用户设置不下载评论

阅读全文