

WooYun.org

已关注 7.7万

[首页](#)
[厂商列表](#)
[白帽子](#)
[团队](#)
[漏洞列表](#)
[提交漏洞](#)
[厂商活动](#)
[企业招聘](#)
[乌云集市](#)
[公告](#)

当前位置: [WooYun](#) >> [漏洞信息](#)

漏洞概要

关注数(23) | [关注此漏洞](#)

缺陷编号: **WooYun-2014-50839**

漏洞标题：手把手教你获取wdCP主机管理系统的PHP源代码

相关厂商：[wdlinux](#)

漏洞作者：**狂小子**

提交时间：2014-02-13 15:45

漏洞类型：敏感信息泄露

危害等级：高

自评Rank：20

漏洞状态： 厂商已经确认

漏洞来源：<http://www.wooyun.org>

Tags标签: **wdCP源码泄漏**

分享漏洞： 分享到 0

4人收藏

漏洞详情

披露状态：

2014-02-13： 细节已通知厂商并且等待厂商处理中

2014-02-14：厂商已经确认，细节仅向厂商公开

2014-02-17： 细节向第三方安全合作伙伴开放

2014-02-24：细节向核心白帽子及相关领域专家公开

2014-03-06：细节向普通白帽子公开

简要描述：

获取源代码后可通过阅读源代码查找是否存在漏洞，万一找到漏洞危害性还是比较大的。

详细说明：

wdCP是WDlinux Control Pane的简称,是一套通过WEB控制和管理服务器的Linux服务器管理系统以及虚拟主机管理系统,旨在易于使用Linux系统做为我们的网站服务器系统,以及平时对Linux服务器的常用管理操作,均可在wdCP的后台里操作完成。

wdCP是使用PHP语言开发并对PHP文件进行加密，需要php_wdcpm.so扩展解析。

其实这次的方法很简单，此方法对一些类似的PHP文件加密也有效，下面来看操作(以index.php文件为例)。

1、查看服务器上的/www/wdlinux/wdcp/index.php文件内容，确实是加密的

```
[root@wdos ~]# cat /www/wdlinux/wdcp/index.php
WATWDCPM鮑J鯨訖vt块qh<uk壘
M壘鉛<搥 JAhq癩0Y'*z膳Y齋掟铈
緬貞B@ 鈿; 搢跡病M襍-翻坏* 烙1薩窰迨磁稅賴L娼root@wdos ~]#
```

2、浏览器访问下wdCP控制面板并查看浏览器中的html源码，这一切都正常。



- 3、编辑服务器上的/www/wdlinux/wdphp/lib/php.ini文件，这个文件正是wdCP运行PHP环境所使用的配置文件，关闭short_open_tag配置项

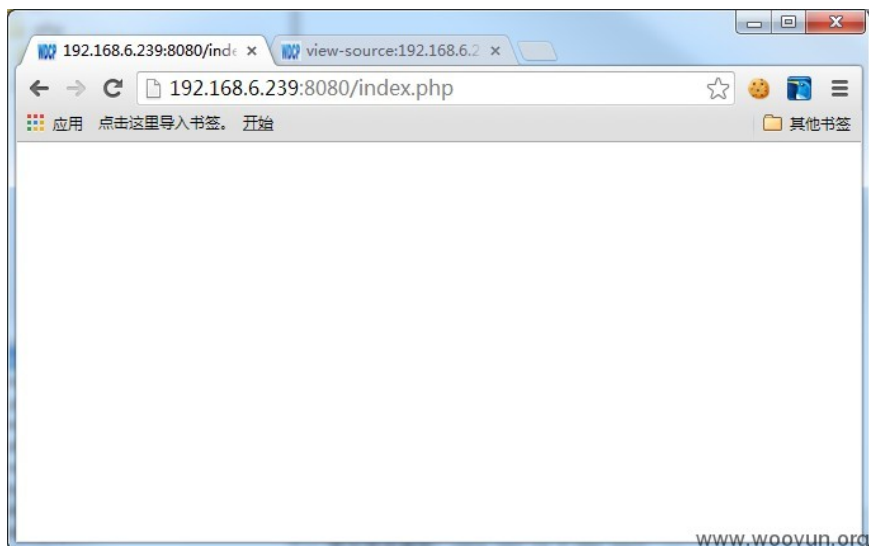
```
; be supported on the ca
; be sure not to use shor
short_open_tag = On
; Allow ASP-style <% %> t
```

改成

```
; be supported on the ca
; be sure not to use sho
short_open_tag = off
; Allow ASP-style <% %>
```

- 4、重启服务，命令： /www/wdlinux/tools/httpd_restart.sh

5、再回浏览器访问下wdCP控制面板并查看浏览器中的html源码，出现白页，html源码中漏出了php源码。



漏洞证明：



修复方案：

在写PHP代码时，不要使用php的短标签，即 <? 改为 <?php 后再对文件加密

版权声明：转载请注明来源 狂小子@乌云

漏洞回应

厂商回应：

危害等级：高

漏洞Rank：20

确认时间：2014-02-14 11:26

厂商回复：

很严重

最新状态：

暂无

漏洞评价：

对本漏洞信息进行评价，以更好的反馈信息的价值，包括信息客观性，内容是否完整以及是否具备学习价值

漏洞评价(共0人评价):

评论

2014-02-13 16:03 hacker@sina.cn (普通白帽子 Rank:222 漏洞数:20 我这人没什么羞耻心，所以请不要跟我装正经...)	0
mark	1#
2014-02-14 11:38 Coody (普通白帽子 Rank:786 漏洞数:90 @乌云)	0
这个必须mark	2#
2014-02-14 14:14 小川 (普通白帽子 Rank:735 漏洞数:153 3月等着我！)	0
坐等公开	3#
2014-02-17 16:29 雨 。(普通白帽子 Rank:169 漏洞数:25 这家伙太懒了 什么都没留下。)	0
低调求一份	4#

验证码

RQ5F

发表评论