

6

1

2

1

[MYSQL] 漏扫发现驱动存在漏洞, 怎么快速查找客户端的驱动版本呢?

原创

大大刺猬

2025-03-20

217

导读

有这么一个场景：
漏扫发现一些mysql的漏洞, 有server层的, 也有驱动层的. server层升级成本太高, 周期较长. 故可以先处理一下驱动相关的漏洞. 比如存在这么一个漏洞:[CVE-2025-21548](#)

CNA: Oracle

Published: 2025-01-21Updated: 2025-01-21

Description

Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/Python). Supported versions that are affected are 9.1.0 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Connectors accessible data as well as unauthorized read access to a subset of MySQL Connectors accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors. CVSS 3.1 Base Score 6.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:H/A:H).

CVSS

1 Total

Learn more

Score	Severity	Version	Vector String
6.4	MEDIUM	3.1	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:H/A:H

Product Status

Learn more

Vendor

Oracle Corporation

Product

MySQL Connectors

Versions

1 Total

Default Status: unknown

Affected

affected through 9.1.0

References

1 Total

oracle.com: Oracle Advisory

vendor-advisory

这个漏洞影响驱动版本小于等于 9.1.0的, 造成的影响是DOS. 具体咋个实现的, 咱也不需要知道, 我们只需要找到有这个漏洞的客户端并做好相关处理即可.

查找客户端的驱动版本

我们要查找客户端的驱动版本, 大概有如下3条路可选:

- 最原始的办法就是找开发问, 但周期可能太长, 而且可能存在遗漏的情况.
- 找漏扫的人要相关的客户端地址信息, 估计不会给(也可能没有)
- 自个在服务端查找客户端驱动版本信息.

前两者不太容易走, 我们就选择最后一条(作为一个DBA, 自个在服务端查找客户端驱动版本信息还不是手到擒来, 前提是有这么个信息).

验证 客户端已发送驱动版本信息

回顾下以前的mysql连接相关知识:

大大刺猬

关注

146

文章

108

粉丝

66K+

浏览量

获得了 350 次点赞

内容获得 70 条评论

获得了 257 次收藏

TA的专栏

PYTHON解析MYSQL

收录 59 篇内容

热门文章

MYSQL 文件解析 (3) 数据文件(ibd)解析

2023-04-232801浏览

ibd2sql解析ibd文件为SQL

2023-04-272060浏览

[MYSQL] 数据恢复, 无备份, 只剩一个 ibd 文件 怎么恢复数据?

2024-04-121948浏览

MYSQL 文件解析 (1) binlog 文件解析

2023-04-231708浏览

mysql-5.7.38启动流程源码解读

2022-09-261529浏览

在线实训环境入口

MySQL在线实训环境

[查看详情 >](#)

最新文章

[MYSQL] 修改字段长度的时候不能使用instant算法? 其实inplace就够了

2025-07-3049浏览

[MYSQL] 修改字段长度的时候不能使用instant算法? 那就定制一个?

2025-07-2581浏览

[MYSQL] row_format=compressed的存储结构浅析

2025-07-1855浏览

[MYSQL] 备份失败,但是啥日志信息都没有

2025-07-1572浏览

[MYSQL] 从库 io_thread 接受binlog速度太慢?

Captured by FireShot Pro: 12 8月 2025, 09:51:18
https://getfireshot.com

果然找到了 performance_schema.session_connect_attrs 和 performance_schema.session_account_connect_attrs 比较复合我们预期.

```
(root@127.0.0.1) [(none)]> select TABLE_SCHEMA, TABLE_NAME, COLUMN_NAME from information
%%attr%' or column_name like '%attr%') and table_schema in ('sys','mysql','performance
+-----+-----+-----+
| TABLE_SCHEMA | TABLE_NAME | COLUMN_NAME |
+-----+-----+-----+
| information_schema | COLLATIONS | PAD_ATTRIBUTE |
| information_schema | COLUMNS_EXTENSIONS | ENGINE_ATTRIBUTE |
| information_schema | COLUMNS_EXTENSIONS | SECONDARY_ENGINE_ATTRIBUTE |
| information_schema | TABLE_CONSTRAINTS_EXTENSIONS | ENGINE_ATTRIBUTE |
| information_schema | TABLE_CONSTRAINTS_EXTENSIONS | SECONDARY_ENGINE_ATTRIBUTE |
| information_schema | TABLES_EXTENSIONS | ENGINE_ATTRIBUTE |
| information_schema | TABLES_EXTENSIONS | SECONDARY_ENGINE_ATTRIBUTE |
| information_schema | TABLESPACES_EXTENSIONS | ENGINE_ATTRIBUTE |
| performance_schema | session_connect_attrs | PROCESSLIST_ID |
| performance_schema | session_connect_attrs | ATTR_NAME |
| performance_schema | session_connect_attrs | ATTR_VALUE |
| performance_schema | session_connect_attrs | ORDINAL_POSITION |
| performance_schema | session_account_connect_attrs | PROCESSLIST_ID |
| performance_schema | session_account_connect_attrs | ATTR_NAME |
| performance_schema | session_account_connect_attrs | ATTR_VALUE |
| performance_schema | session_account_connect_attrs | ORDINAL_POSITION |
| information_schema | USER_ATTRIBUTES | ATTRIBUTE |
| mysql | user | User_attributes |
+-----+-----+-----+
```

查阅[官网](#), 发现前者更符合我们的期望. 查看该表信息:

```
(root@127.0.0.1) [(none)]> select * from performance_schema.session_connect_attrs;
+-----+-----+-----+-----+
| PROCESSLIST_ID | ATTR_NAME | ATTR_VALUE | ORDINAL_POSITION |
+-----+-----+-----+-----+
| 17 | _pid | 13371 | 0 |
| 17 | _platform | x86_64 | 1 |
| 17 | _os | Linux | 2 |
| 17 | _client_name | libmysql | 3 |
| 17 | os_user | root | 4 |
| 17 | _client_version | 8.0.28 | 5 |
| 17 | program_name | mysql | 6 |
| 23 | _pid | 15571 | 0 |
| 23 | _platform | x86_64 | 1 |
| 23 | _client_version | 8.0.28 | 2 |
| 23 | _os | Linux | 3 |
| 23 | _client_name | libmysql | 4 |
| 23 | _source_host | ddcw21 | 5 |
| 23 | _connector_version | 8.0.28 | 6 |
| 23 | _connector_license | GPL-2.0 | 7 |
| 23 | _connector_name | mysql-connector-python | 8 |
+-----+-----+-----+-----+
```

客户端驱动版本信息这不就来了么, 还有processlist_id, 我们稍微关联下表就能 查询到 驱动版本低于9.1.0的连接了.

```
select a.id,a.user,a.host,a.db,b.ATTR_NAME,b.ATTR_VALUE,b.ORDINAL_POSITION from information
-----

(root@127.0.0.1) [(none)]> select a.id,a.user,a.host,a.db,b.ATTR_NAME,b.ATTR_VALUE,b.ORDINAL_POSITION from information schema.
processlist as a left join (select * from performance_schema.session_connect_attrs where ATTR_NAME='_connector_version' and AT
TR_VALUE <= '9.1.0' and PROCESSLIST_ID in (select PROCESSLIST_ID from performance_schema.session_connect_attrs where ATTR_NAME
='_connector_name' and ATTR_VALUE='mysql-connector-python')) as b on a.id=b.processlist_id where b.ATTR_NAME is not null;
+-----+-----+-----+-----+-----+-----+-----+
| id | user | host | db | ATTR_NAME | ATTR_VALUE | ORDINAL_POSITION |
+-----+-----+-----+-----+-----+-----+-----+
| 23 | root | ddcw21:37746 | db1 | _connector_version | 8.0.28 | 6 |
+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.01 sec)

(root@127.0.0.1) [(none)]> █
```

吼吼, 我们找到了客户端的驱动版本信息, 那问题又来了, 怎么修复呢?

我这里只考虑了python版的驱动 ATTR_VALUE='mysql-connector-python' 实际使用时, 根据自己情况来调整.

漏洞处理

要处理这个漏洞的话, 最稳妥的方法就是老老实实的升级, 但我是谁啊, 能老实吗? 或者修改驱动版本信息

升级的话, 周期太长, 而且还可能存在兼容性问题. 所以我们选择后者, 修改驱动包的版本信息... 以python版的驱动mysql-connector-python为例. 我们只需要编辑文件 `mysql/connector/version.py` 修改里面的版本信息如下:

```
VERSION = (9, 9, 99, '', 1)
```

然后重启应用(不管选哪种都涉及到应用重启)再次查看, 发现驱动版本已更新(新得不得了)

```
(root@127.0.0.1) [(none)]> select * from performance_schema.session_connect_attrs;
```

PROCESSLIST_ID	ATTR_NAME	ATTR_VALUE	ORDINAL_POSITION
27	_pid	13371	0
27	_platform	x86_64	1
27	_os	Linux	2
27	_client_name	libmysql	3
27	os_user	root	4
27	_client_version	8.0.28	5
27	program_name	mysql	6
28	_pid	16441	0
28	_platform	x86_64	1
28	_client_version	8.0.28	2
28	_os	Linux	3
28	_client_name	libmysql	4
28	source_host	ddcw21	5
28	connector_version	9.9.99	6
28	connector_license	GPL-2.0	7
28	connector_name	mysql-connector-python	8

16 rows in set (0.00 sec)

这下看它还能不能扫出漏洞 -_-

总结

这种影响不大的漏洞, 通常不需要管, 非要管的话, 注意做好相关测试, 尤其是兼容性(稳定性可能不好测). 如果不能升级, 又想解决漏洞的话, 就只有修改客户端服务端的版本了(前提是数据库服务器一定得在内网, 应用账号的权限也要最小化控制).(屏蔽漏扫也是不错的选择)

本文涉及到的知识和脚本都是之前的内容, 有兴趣的可以自己翻一翻以前的文章.

参考:

<https://www.cve.org/CVERecord?id=CVE-2025-21548>

<https://www.oracle.com/security-alerts/cpujan2025.html>

<https://dev.mysql.com/doc/refman/8.0/en/performance-schema-session-account-connect-attrs-table.html>

<https://dev.mysql.com/doc/refman/8.0/en/performance-schema-session-connect-attrs-table.html>

墨力计划 mysql

「喜欢这篇文章，您的关注和赞赏是给作者最好的鼓励」

关注作者

赞赏

【版权声明】本文为墨天轮用户原创内容，转载时必须标注文章的来源（墨天轮），文章链接，文章作者等基本信息，否则作者和墨天轮有权追究责任。如果您发现墨天轮中有涉嫌抄袭或者侵权的内容，欢迎发送邮件至：contact@modb.pro进行举报，并提供相关证据，一经查实，墨天轮将立刻删除相关内容。

评论

分享你的看法，一起交流吧~



咚咚 LV.5

[MYSQL] 漏扫发现驱动存在漏洞, 怎么快速查找客户端的驱动版本呢?

4月前 点赞 评论



luyingjun LV.4

[MYSQL] 漏扫发现驱动存在漏洞, 怎么快速查找客户端的驱动版本呢?

4月前 点赞 评论

相关阅读

ACDU周度精选 | 本周数据库圈热点 + 技术干货分享 (2025/7/25期)
墨天轮小助手 470次阅读 2025-07-25 15:54:18

ACDU周度精选 | 本周数据库圈热点 + 技术干货分享 (2025/7/17期)
墨天轮小助手 436次阅读 2025-07-17 15:31:18

墨天轮「实操看我的」数据库主题征文活动启动
墨天轮编辑部 379次阅读 2025-07-22 16:11:27

深度解析MySQL的半连接转换
听见风的声音 205次阅读 2025-07-14 10:23:00

MySQL 9.4.0 正式发布，支持 RHEL 10 和 Oracle Linux 10
严少安 199次阅读 2025-07-23 01:21:32

索引条件下推和分区——一条SQL语句执行计划的分析
听见风的声音 197次阅读 2025-07-23 09:22:58

null和子查询——not in和not exists怎么选择？
听见风的声音 182次阅读 2025-07-21 08:54:19

MySQL数据库SQL优化案例(走错索引)
陈举超 166次阅读 2025-07-17 21:24:40

使用 MySQL Clone 插件为MGR集群添加节点
黄山谷 163次阅读 2025-07-23 22:04:19

MySQL 8.0.40：字符集革命、窗口函数效能与DDL原子性实践
shunwah  141次阅读 2025-07-15 15:27:19