CVE-2026-3494

Affected Software	MariaDB
CVSS Score	5.3
ID	3
Published Date	March 3, 2026
비고	CVE 내용과 일치하지 않아, MariaDB에 문의예정
소프트웨어 버전(PoC)	10.3.39 / 11.8.5 / 11.8.6
테스트 환경(PoC)	Rocky Linux 8.10

https://www.cve.org/CVERecord?id=CVE-2026-3494

Vulnerability_Published_Date

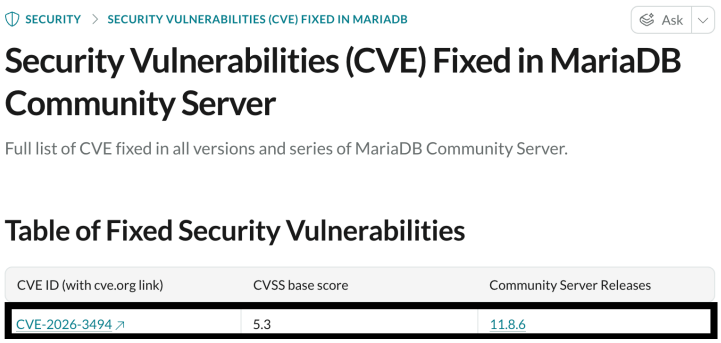
- 2025-04-15

Affected Software & version

CVE.org

- Software : MySQL Cluster(cve.org)
- Unaffected Version
  - unaffected at **10.6.25**
  - unaffected at **10.11.16**
  - unaffected at **11.4.10**
  - unaffected at **11.8.6**

MariaDB.org


SECURITY > SECURITY VULNERABILITIES (CVE) FIXED IN MARIADB

Ask

Security Vulnerabilities (CVE) Fixed in MariaDB Community Server

Full list of CVE fixed in all versions and series of MariaDB Community Server.

Table of Fixed Security Vulnerabilities

CVE ID (with cve.org link)	CVSS base score	Community Server Releases
CVE-2026-3494	5.3	11.8.6

취약점 설명 (Vulnerability description)

- MariaDB Server 11.8.5 버전 까지, server_audit 플러그인이 활성화 되어 있으며, server_audit_events가 `QUERY_DCL, QUERY_DDL, QUERY_DML` 로 필터링 되도록 설정되어 있으면
  - 데이터베이스의 인증된 사용자가 주석이 붙은 (`이중 하이픈(–) 또는 해시(#)`)

    - SQL 문장을 호출하면 해당 문장은 기록되지 않는다
- In MariaDB server version through 11.8.5, when server audit plugin is enabled with server_audit_events variable configured with QUERY_DCL, QUERY_DDL, or QUERY_DML filtering, if an authenticated database user invokes a SQL statement prefixed with double-hyphen (—) or hash (#) style comments, the statement is not logged.

PoC Environment (26.04.10 00:54)

- OS : Rocky Linux 8.10
- DBMS : `MariaDB 10.3.39` vs `MariaDB 11.8.6` vs `MariaDB 11.8.5`

PoC 공격조건

1. `server_audit` Plugin이 설치 되어있어야 하며, 해당 플러그인을 통해 감사로그를 기록하고 있어야 함
   The `server_audit` plugin must be installed, and audit logging must be enabled through this plugin.
2. `server_audit_events` 는 `QUERY_DCL, QUERY_DML, QUERY_DDL` 로 필터링 되어있어야 함
   `server_audit_events` must be configured to filter `QUERY_DCL`, `QUERY_DML`, and `QUERY_DDL`.

기본 설정

▼ `server_audit plugin` 검색
Find `server_audit plugin`

```
# MariaDB 10.3.39 & 11.8.6 & 11.8.5
MariaDB [(none)]> show variables like 'plugin_dir';
+---------------+-------------------------+
| Variable_name | Value                   |
+---------------+-------------------------+
| plugin_dir    | /usr/lib/mysql/plugin/ |
+---------------+-------------------------+
1 row in set (0.001 sec)

MariaDB [(none)]> exit
Bye

# MariaDB 10.3.39
root@77f802a94157:/var/lib/mysql# ls -al /usr/lib/mysql/plugin | grep server_audit.so
-rw-r--r--. 1 root root  68080 May  3  2023 server_audit.so

# MariaDB 11.8.6
root@67aec2205de2:/var/lib/mysql# ls -al /usr/lib/mysql/plugin | grep server_audit.so
-rw-r--r--. 1 root  root  66432 Jan 31 16:12 server_audit.so

# MariaDB 11.8.5
root@90bb7eb5918d:/var/lib/mysql# ls -al /usr/lib/mysql/plugin | grep server_audit.so
-rw-r--r--. 1 root  root  77120 Nov 13 10:19 server_audit.so
```

▼ `server_audit plugin` 설치
Install `server_audit plugin`

```
# MariaDB 10.3.39 & 11.8.6 & 11.8.5

MariaDB [(none)]> install plugin server_audit soname 'server_audit.so';
Query OK, 0 rows affected (0.021 sec)
```

▼ server_audit 플러그인 사용 및 이벤트 설정
Use the `server_audit plugin` and configure events

```
# MariaDB 10.3.39 & 11.8.6 & 11.8.5

MariaDB [(none)]> set global server_audit_logging=ON;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> set global server_audit_events='QUERY_DCL,QUERY_DDL,QUERY_DML';
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> set global server_audit_output_type=FILE;
Query OK, 0 rows affected (0.000 sec)
```

▼ 로그파일명 확인
Check Logfile Name

```
# MariaDB 10.3.39 & 11.8.6 & 11.8.5

MariaDB [(none)]> show variables like 'server_audit_file_path';
+------------------------+------------------+
| Variable_name          | Value            |
+------------------------+------------------+
| server_audit_file_path | server_audit.log |
+------------------------+------------------+
1 row in set (0.002 sec)
```

Execute PoC

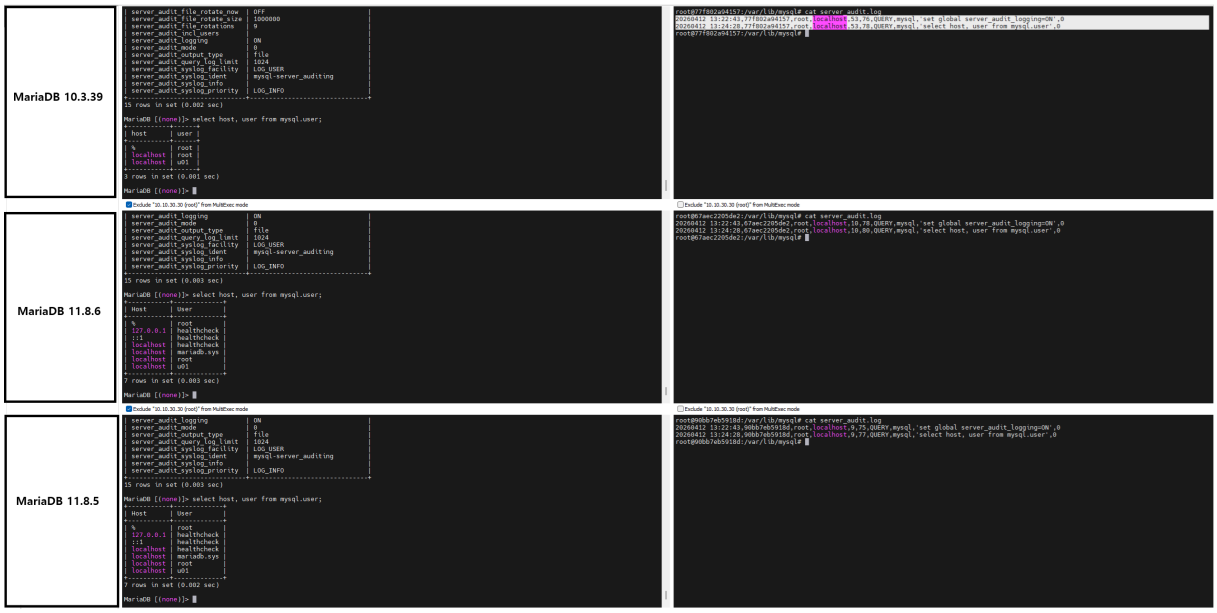
Version : (10.3.39) vs (11.8.6) vs (11.8.5)

▼ Query 실행 및 로그 확인 (정상 실행 Query) - Test Case 1
Execute query and check logs (successfully executed query) - Test Case 1

```
MariaDB [(none)]> select host, user from mysql.user;
+-----------+------+
| host      | user |
+-----------+------+
| %         | root |
| localhost | root |
+-----------+------+
2 rows in set (0.001 sec)
```

```
# MariaDB 10.3.39
20260412 13:24:28,77f802a94157,root,localhost,53,78,QUERY,mysql,'select host, user from my
sql.user',0
```

```
# MariaDB 11.8.6
20260412 13:24:28,67aec2205de2,root,localhost,10,80,QUERY,mysql,'select host, user from my
sql.user',0

# MariaDB 11.8.5
20260412 13:24:28,90bb7eb5918d,root,localhost,9,77,QUERY,mysql,'select host, user from mys
ql.user',0
```



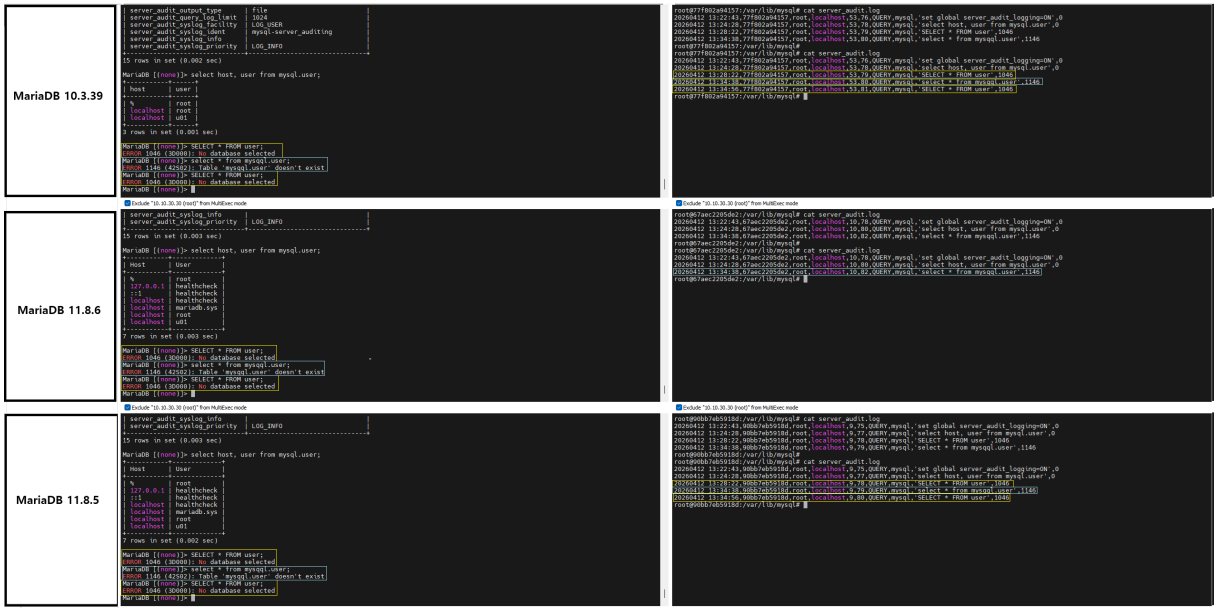
▼ Query 실행 및 로그 확인 (에러 발생 Query) - Test Case 2
Execute query and check logs (query that causes an error) - Test Case 2

- (KOR) MariaDB 11.8.6 버전에서는 1046 Error 로그에 대해 기록되지 않음
- (ENG) In MariaDB 11.8.6, Error 1046 is not recorded in the logs.

```
MariaDB [(none)]> SELECT * FROM user;
ERROR 1046 (3D000): No database selected

MariaDB [(none)]> SELECT * FROM mysqql.user;
ERROR 1146 (42S02): Table 'mysqql.user' doesn't exist
```

```
# MariaDB 10.3.39
20260412 13:28:22,77f802a94157,root,localhost,53,79,QUERY,mysql,'SELECT * FROM user',1046
20260412 13:34:38,77f802a94157,root,localhost,53,80,QUERY,mysql,'select * from mysqql.use
r',1146

# MariaDB 11.8.6
20260412 13:34:38,67aec2205de2,root,localhost,10,82,QUERY,mysql,'select * from mysqql.use
r',1146

# MariaDB 11.8.5
20260412 13:34:38,90bb7eb5918d,root,localhost,9,79,QUERY,mysql,'select * from mysqql.use
```

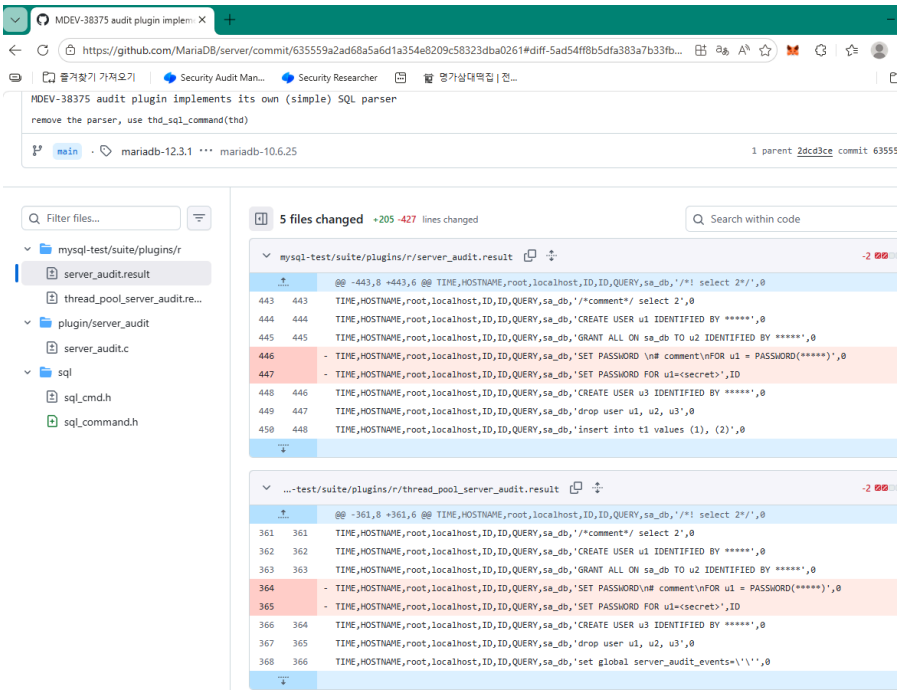
```
r',1146
20260412 13:34:56,90bb7eb5918d,root,localhost,9,80,QUERY,mysql,'SELECT * FROM user',1046
```



▼ Query 실행 및 로그 확인 (Github Example Query) #1 - Test Case 3

Execute query and check logs (Github Example Query) #1 - Test Case 3

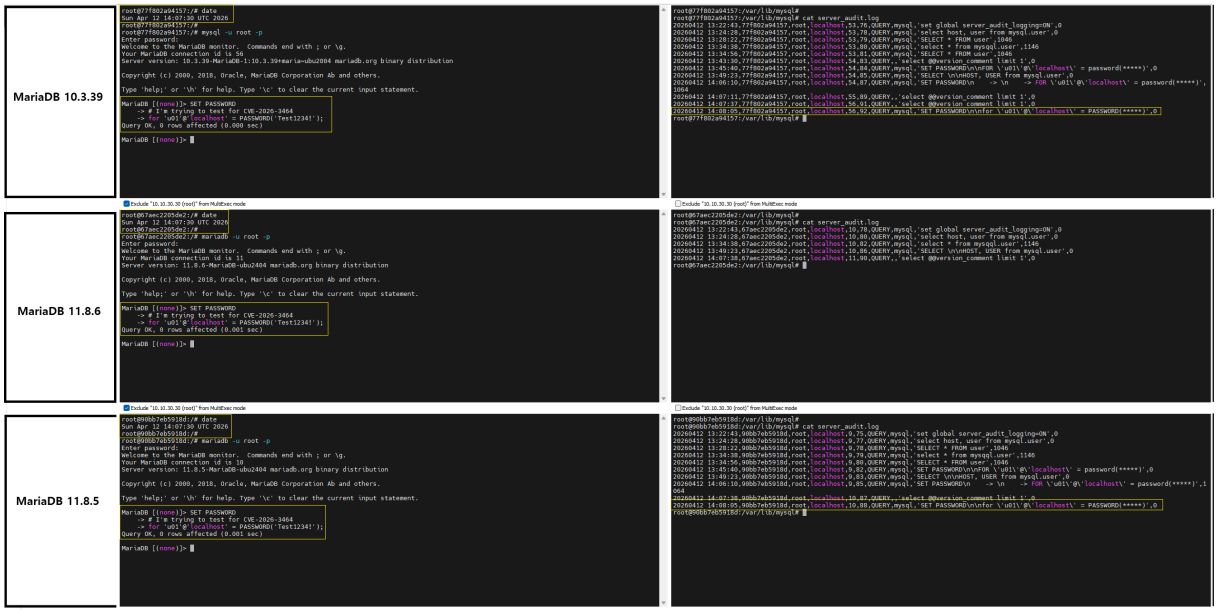
- https://github.com/MariaDB/server/commit/635559a2ad68a5a6d1a354e8209c58323dba0261




```
MariaDB [(none)]> SET PASSWORD
    -> # I'm trying to test for CVE-2026-3464
```

```
    -> FOR 'u01'@'localhost' = password('Test1234!');
Query OK, 0 rows affected (0.001 sec)
```

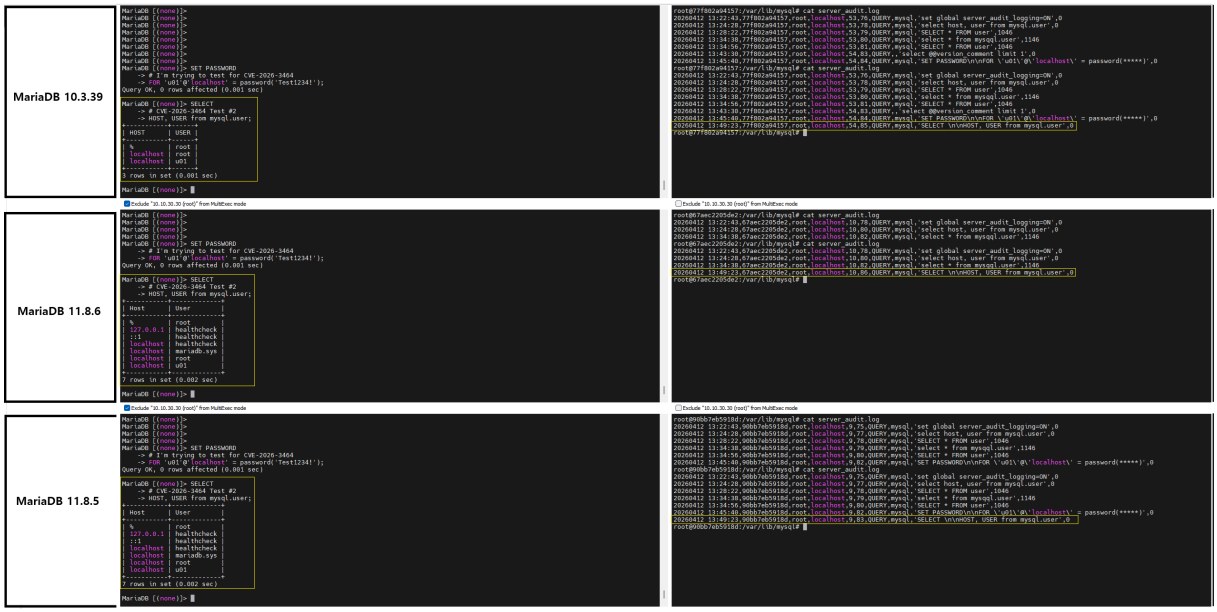
```
# MariaDB 10.3.39
20260412 14:08:05,77f802a94157,root,localhost,56,92,QUERY,mysql,'SET PASSWORD\n\nfor \'u01
\'@\'localhost\' = PASSWORD(*****)',0

# MariaDB 11.8.6
   # 기록되지 않음
   # Not Record

# MariaDB 11.8.5

20260412 14:08:05,90bb7eb5918d,root,localhost,10,88,QUERY,mysql,'SET PASSWORD\n\nfor \'u01
\'@\'localhost\' = PASSWORD(*****)',0
```



▼ Query 실행 및 로그 확인 (Github Example Query) #2 - Test Case 4
Execute query and check logs (Github Example Query) #2 - Test Case 4

```
MariaDB [(none)]> SELECT
    -> # CVE-2026-3464 Test #2
    -> HOST, USER from mysql.user;
+-----------+------+
| HOST      | USER |
+-----------+------+
| %         | root |
| localhost | root |
| localhost | u01  |
+-----------+------+
3 rows in set (0.001 sec)
```

```
# MariaDB 10.3.39
20260412 13:49:23,77f802a94157,root,localhost,54,85,QUERY,mysql,'SELECT \n\nHOST, USER fro
m mysql.user',0

# MariaDB 11.8.6
20260412 13:49:23,67aec2205de2,root,localhost,10,86,QUERY,mysql,'SELECT \n\nHOST, USER fro
m mysql.user',0

# MariaDB 11.8.5
20260412 13:49:23,90bb7eb5918d,root,localhost,9,83,QUERY,mysql,'SELECT \n\nHOST, USER from
mysql.user',0
```



※ 이미지 내 포함된 Comment “2026-3464” 는 오타
※ The comment “2026-3464” included in the image is a typo.

실행 결과 (Execution result)

- (Test Case 1) 정상적으로 실행한 쿼리에 대해서는 server_audit 를 통해 로그가 남는 것으로 판단됨
  (Test Case 1) Queries executed normally are confirmed to be logged through `server_audit`.
  - `SELECT HOST, USER FROM mysql.user;`

- (Test Case 2) 에러 발생을 유도한 쿼리에 대해 MariaDB 11.8.6 버전에서 `1046 Error` 가 기록되지 않음
  (Test Case 2) For queries that intentionally trigger errors, Error 1046 is not recorded in MariaDB 11.8.6.
  - `SELECT HOST, USER FROM user;`
  - MariaDB 10.3.39 , MariaDB 11.8.5 에서는 기록이 되어지는 것을 확인
    It is confirmed that this error is recorded in MariaDB 10.3.39 and MariaDB 11.8.5,
  - MariaDB 11.8.6 에서는 기록이 되지 않는 것을 확인
    but not recorded in MariaDB 11.8.6.

- (Test Case 3) CVE 및 Github에서 공개한 이중 하이픈(—) 혹은 해시(#) 를 포함해서 SET 구문을 실행
  (Test Case 3) When executing `SET` statements containing double hyphens (`--`) or hash (`#`) as disclosed in the CVE and GitHub,
  - MariaDB 11.8.6 에서는 로그가 기록되지 않음
    logs are not recorded in MariaDB 11.8.6,
  - MariaDB 11.8.5 / MariaDB 10.3.39 에서는 로그가 기록됨
    while they are recorded in MariaDB 11.8.5 and MariaDB 10.3.39.

```
MariaDB [(none)]> SET PASSWORD
    -> # I'm trying to test for CVE-2026-3464
    -> for 'u01'@'localhost' = PASSWORD('Test1234!');
Query OK, 0 rows affected (0.000 sec)
```

- (Test Case 4) CVE 및 Github에서 공개한 이중 하이픈(—) 혹은 해시(#) 를 포함해서 SELECT 구문 실행
  (Test Case 4) When executing `SELECT` statements containing double hyphens (`--`) or hash (`#`) as disclosed in the CVE and GitHub,
  - MariaDB 10.3.39, MariaDB 11.8.6, MariaDB 11.8.5에서 모두 로그를 남김
    logs are recorded in all tested versions: MariaDB 10.3.39, MariaDB 11.8.6, and MariaDB 11.8.5.

```
MariaDB [(none)]> SELECT
    -> # CVE-2026-3464 Test #2
    -> HOST, USER from mysql.user;
```

결론(Conclusion)

- CVE에서 공개한 내용에 의하면, MariaDB 11.8.5 버전까지
  According to the details disclosed in the CVE, up to MariaDB version 11.8.5,
  - server_audit 플러그인을 사용하면서
    when using the `server_audit` plugin,
  - server_audit_events 가 `QUERY_DCL, QUERY_DDL, QUERY_DML` 로 설정되어 있다면
    and with `server_audit_events` configured as `QUERY_DCL`, `QUERY_DDL`, and `QUERY_DML`,
    - 이중 하이픈이나 해시를 통한 comments 사용 시 로그가 기록되지 않을 수 있다는 내용이 맞지 않음
      it is stated that logs may not be recorded when comments using double hyphens (`--`) or hash (`#`) are used — however, this is not entirely accurate.

> **Description**
>
> In MariaDB server version through 11.8.5, when server audit plugin is enabled with server_audit_events variable configured with QUERY_DCL, QUERY_DDL, or QUERY_DML filtering, if an authenticated database user invokes a SQL statement prefixed with double-hyphen (—) or hash (#) style comments, the statement is not logged.

- **MariaDB 10.3.39**
  - 이 버전은 CVE 취약점 공개일 이전에 보안 패치가 지원이 되었기 때문에 테스트 해본 것이며,
    This version was tested because it had already received security patches prior to the CVE disclosure date,
    - 4가지 테스트에 대해 모두 로그가 남고 있음
      and in all four test cases, logs were successfully recorded.

- **MariaDB 11.8.5**
  - CVE.org 에서 공개한 버전인 11.8.5에 대해 테스트 결과,
    However, testing results on version 11.8.5, as disclosed on CVE.org, show that:
    - 4가지 테스트에 대해 모두 로그가 남고 있음
      and in all four test cases, logs were successfully recorded.

- **MariaDB 11.8.6**
  - Mariadb.org 에서 조치되었다고 작성된 버전이며,
    this is the version noted as patched on MariaDB.org, but
    - **Test Case 2에 대해서 1046 Error가 기록되지 않음**
      in Test Case 2, Error 1046 is not recorded,
    - **Test Case 3에 대해서 이중하이픈, 해시를 포함한 `SET` 구문에 대해 로그가 기록되지 않음**
      in Test Case 3, logs are not recorded for `SET` statements containing double hyphens or hash comments,
    - **Test Case 4에 대해서 이중하이픈, 해시를 포함한 `SELECT` 구문에 대해 로그가 기록됨**
      and in Test Case 4, logs are recorded for `SELECT` statements containing double hyphens or hash comments.

- MariaDB 에서 조치되었다고 한 11.8.6 버전에 대해 일부 로그가 기록되지 않고 있으며,
  In MariaDB 11.8.6, which is stated as fixed, some logs are not being recorded,
  - 오히려 11.8.5 버전을 포함한 보안지원이 종료된 버전에서 기록이 되고있음
    whereas in older versions—including 11.8.5 and even end-of-life versions—those logs are properly recorded.

- 제가 테스트를 잘못했을 수 있습니다.
  I may have conducted the tests incorrectly.
- 만약 그렇다면 피드백을 주시기 바랍니다.
  If so, I would appreciate your feedback.