

Overall Rating - Critical



This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of an improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache InLong from 1.4.0 to 1.7.0.

Technical Details

In the `toAuditCkSql` method, the `groupId`, `streamId`, `auditId`, and `dt` are directly concatenated into the SQL query statement, which may lead to SQL injection attacks. Users are advised to upgrade to Apache InLong's 1.8.0.

This vulnerability is rated as a **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- Ensure mitigation is performed as soon as possible.

Please notify [VRM](#) with any questions or concerns you may have.

References

- [CVE-2023-35088](#)
- <https://github.com/apache/inlong/pull/8198>
- <http://seclists.org/fulldisclosure/2023/Jul/43>
- <http://www.openwall.com/lists/oss-security/2023/07/25/4>
- <https://lists.apache.org/thread/os7b66x4n8dbtrdpb7c6x37bb1vjb0tk>