安全通告

关于 MySQL2 readCodeFor 存在远程代码执行漏洞预警通告

发布日期：2024-4-24

[2024]008 号

漏洞描述

2024 年 4 月 24 日公司监测到关于 MySQL2 readCodeFor 存在远程代码执行漏洞（CVE-2024-21508）。MySQL2 是用于操作 MySQL 数据库的高性能 Node.js 库，可兼容 Node MySQLAPI、并提供预编译语句、扩展编码等功能。由于 readCodeFor 函数中未正确验证 supportBigNumbers 和 bigNumberStrings 值,威胁者可通过构造恶意对象并将其作为参数传递给 connection.query 函数来执行恶意 JavaScript 代码,从而导致远程代码执行。

漏洞编号

CVE-2024-21508

漏洞危害

攻击者可通过构造恶意对象并将其作为参数传递给 connection.query 函数来执行恶意 JavaScript 代码,从而导致远程代码执行。

漏洞等级

高危

受影响版本

mysql2(npm) < 3.9.4

修复方案

目前该漏洞已经修复,受影响用户可更新到 mysql2 3.9.4 或更高版本。

下载链接：

https://github.com/sidorares/node-mysql2/releases

参考链接

https://github.com/sidorares/node-mysql2/pull/2572