ONEStor是否涉及PostgreSQL 权限提升漏洞(CVE-2016-5424)

孟小涛 2022-09-23 发表

漏洞相关信息

漏洞编号： CVE-2016-5424

漏洞名称： PostgreSQL 权限提升漏洞

产品型号及版本： ONEStor

漏洞描述

在PostgreSQL客户端程序处理包含换行符、回车符、双引号或反斜杠的数据库和角色名的方式中发现了一个缺陷。通过构造这样的对象名称，当超级用户下次执行对脆弱客户机程序的维护时，具有CREATEDB或CREATEROLE选项的角色可以将其特权升级为超级用户。

参考资料：https://www.postgresql.org/docs/9.3/release-9-3-14.html

漏洞解决方案

在E3338使用的PG9.3.25已解决该漏洞