ONEStor是否涉及 PostgreSQL 空指针间接引用远程代码执行漏洞(CVE-2016-5423)

孟小涛 2022-09-23 发表

漏洞相关信息

漏洞编号： CVE-2016-5423

漏洞名称： PostgreSQL 空指针间接引用远程代码执行漏洞

产品型号及版本： ONEStor

漏洞描述

在PostgreSQL服务器处理某些包含CASE/WHEN命令的SQL语句的方式中发现了一个缺陷。远程的、经过身份验证的攻击者可以使用专门编写的SQL语句导致PostgreSQL崩溃，或泄露少量服务器内存，或者可能执行任意代码。

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9.3.25已解决该漏洞