ONEStor是否涉及 PostgreSQL SQL注入漏洞(CVE-2018-10915)

对象存储 孟小涛 2022-09-22 发表

漏洞相关信息

漏洞编号： (CVE-2018-10915)
漏洞名称： PostgreSQL SQL注入漏洞
产品型号及版本： ONEStor

漏洞描述

PostgreSQL默认客户端库libpq存在漏洞，libpq无法正确重置连接之间的内部状态。处理步骤如果受影响的libpq版本与来自不受信任输入的“host”或“hostaddr”连接参数一起使用，攻击者就可以绕过客户端连接安全特性，获得对更高特权连接的访问权限，或者通过SQL注入导致PQescape()函数故障，可能造成其他影响。

漏洞解决方案

https://www.postgresql.org/docs/9.3/release-9-3-24.html

根据如上官方描述，PG在9.3.24解决了该问题，ONEStor E3338使用的版本是9.3.25，已解决