ONEStor是否涉及 PostgreSQL 不安全临时文件创建漏洞(CVE-2018-1053)

孟小涛 2022-09-23 发表

漏洞相关信息

漏洞编号： CVE-2018-1053

漏洞名称： PostgreSQL 不安全临时文件创建漏洞

产品型号及版本： ONEStor

漏洞描述

此版本的CloudForms修正了在运行pg_upgrade时调用的一个问题，攻击者可以通过该问题读取或修改当前工作目录中的' pg_dumpall-g '的输出。在这个版本中，任何攻击都是不可行的，因为目录模式阻止入侵者搜索当前工作目录，而主流的umask阻止攻击者打开文件。

漏洞解决方案

在E3338使用的9.3.25已解决该漏洞