云数产品是否涉及ApacheCommons Configuration 远程代码执行漏洞

程鑫 2022-07-19 发表

漏洞相关信息

漏洞编号： CVE-2022-33980

漏洞名称： ApacheCommons Configuration 远程代码执行漏洞

产品型号及版本： CAS&UIS&ONEStor&VDI&CloudOS&大数据&数据库

漏洞描述

Apache Commons Configuration 执行变量插值，允许动态评估和扩展属性。插值的标准格式是“${prefix:name}”，其中“prefix”用于定位执行插值的 org.apache.commons.configuration2.interpol.Lookup 实例。从 2.4 版开始到 2.7 版，默认的 Lookup 实例集包括可能导致任意代码执行或与远程服务器联系的插值器。这些查找是： - “script” - 使用 JVM 脚本执行引擎 (javax.script) 执行表达式 - “dns” - 解析 dns 记录 - “url” - 从 url 加载值，包括来自远程服务器 如果使用了不受信任的配置值，则在受影响的版本中使用插值默认值的应用程序可能容易受到远程代码执行或与远程服务器的无意接触的影响。建议用户升级到 Apache Commons Configuration 2.8.0，默认情况下禁用有问题的插值器。

漏洞解决方案

CAS&UIS&VDI&ONEStor&CloudOS&大数据&数据库均不涉及