中共内蒙古自治区委员会网络安全和信息化委员会办公室
国家计算机网络与信息安全管理中心内蒙古分中心
文件

内党网安通〔2019〕17号

关于“云存储应用存在越权访问和文件上传漏洞”网络安全预警的通报

各盟市及满洲里、二连浩特市委网信办，自治区各有关部门和单位：

近日，国家信息安全漏洞共享平台（CNVD）收录了由腾讯安全玄武实验室发现并报送的云存储应用越权访问和文件上传漏洞（CNVD-2019-37364）。攻击者利用该漏洞，可在越权的情况下，远程读取、修改云存储中的内容。目前，漏洞相关细节未公开，漏洞影响范围和危害较大。

一、漏洞情况分析

云存储是云计算基础上延伸和衍生发展出来的新概念，综合采用分布式处理、并行处理和网格计算等手段，将网络中不同类型的存储设备通过应用软件集合起来协同工作，对外提供统一的数据存储和业务访问功能。云存储在移动APP、

网页版程序、APP 小程序（以下简称云存储应用）等场景得到了广泛应用。用户访问云存储数据时，进行签名请求的密钥有永久密钥和临时密钥两种方式。

腾讯安全玄武实验室研究发现云存储应用由于配置不当，存在越权访问和文件上传漏洞：使用临时密钥进行文件上传的云存储应用，缺乏对文件（存储桶）访问或上传路径（存储桶）的权限限制，导致文件（存储桶）越权访问或文件上传漏洞；使用永久密钥为文件上传请求签名的云存储应用，缺乏对永久密钥的必要保护，产生任意路径文件（存储桶）的越权访问和文件上传漏洞。攻击者利用上述漏洞，通过云存储应用破解或网络抓包获得永久密钥或临时密钥，实现对云存储中的文件数据的窃取，甚至篡改用户保存在云存储中的数据文件。

CNVD 对该漏洞的综合评级为“高危”。

二、漏洞影响范围

漏洞影响情况如下：

腾讯安全玄武实验室阿图因系统分析结果显示，使用国内主流厂商云存储服务的安卓 APP 数量为 4148 个。抽样检测结果显示，受此漏洞影响的应用比例达 70%。CNVD 平台已于 10 月 28 日完成对上述受影响 APP 的云服务厂商通报工作。

三、漏洞处置建议

CNVD 建议云存储应用开发者采用如下方式修复漏洞：

1、采用临时签名上传文件的云存储应用：根据业务场景将服务端生成的临时密钥权限更新至最小，限定文件的上传路径和上传的目标存储桶，去除读文件、列存储桶、列对象、覆盖文件等非业务必要权限。

2、采用永久密钥签名上传文件的云存储应用：更新客户端和服务端上传逻辑，改为用最小权限的临时密钥方式或者 PUT 方式进行上传。

CNVD 建议云存储服务提供商一方面进行漏洞排查，通知云存储用户自查和修复，并提供必要的技术支持；另一方面完善云存储的使用说明文档，提醒云存储用户错误配置可能导致的安全问题，并针对常用场景给出配置策略建议。

请各地区、各有关部门和单位结合自身实际情况及时排查，在确保网络和信息系统安全稳定运行的前提下，按照 CNVD 建议进行处置，避免引发网络安全事件。

联系人及电话：张　宇　0471-3905371

王　艳　0471-4826732

中共内蒙古自治区委员会
网络安全和信息化
委员会办公室

国家计算机网络与信
息安全管理中心
内蒙古分中心

2019 年 11 月 21 日

中共内蒙古自治区委员会网络安全和信息化委员会办公室 2019 年 11 月 21 日印发