**网络安全事件处置报告**

|  |  |  |
| --- | --- | --- |
| 事件基本信息 | 来源 | □监控系统，☑租户报障/投诉，□第三方反馈，□情报  节点： 华南节点 |
| 租户名称 | 139.159.149.185 |
| 事件概要 | 客户报障云主机139.159.149.185 CPU占用100%，请求安全排查。获取授权后排查主机发现恶意挖矿木马。 |
| 详细分析 | 1. 登录主机发现异常进程正在运行，此进程为对外扫描进程，请用户侧核实后自行删除；     另外，主机还存在如下异常进程，此进程为下载挖矿进程，请用户侧核实后自行删除；    二、木马原文件在/tmp/.mas/bin/目录下；    同时在/tmp目录下发现异常文件；     1. 计划任务下发现下载挖矿木马自启动项；      1. 端口扫描发现redis默认端口完全暴露在外网；     根因分析：  在主机/tmp目录下，发现异常redis相关文件，如下图所示：    主机redis为默认配置，存在未授权漏洞，初步判断主机因此漏洞导致被黑客入侵。redis相关漏洞被入侵原理可参考链接：  <http://www.freebuf.com/vuls/85021.html>。 | |
| 事件原因 | 初步判断主机因redis未授权访问认证漏洞被入侵。 | |
| 安全建议 | 1、修改所有OS系统口令（包括管理员和普通用户）、数据库账号口令、应用（WEB）系统管理账号口令为强口令，密码12位以上；  2、禁止不必要的端口直接暴露在公网，设置防火墙规则或配置安全组策略来禁止端口开放情况；非公共开放的业务端口（如22、3306、6379），建议设置只允许特定的IP进行连接；  3、严格控制各服务的系统权限，各服务进程请不要以root权限运行；各应用(如WEB)同数据库交互的账号同样不要使用root权限的账号；  4、建议定期做好数据备份（虚拟机内部备份，异地备份，云上云下备份等），避免被加密勒索。 | |
| 处理人/日期 | 华为云业务部网络安全中心 2018-11-16 | |