H3C关于memcached反射攻击问题应对方案的技术公告

王剑虎 2018-03-07 发表

【漏洞背景】

近日，国家互联网应急中心（CNCERT）通报了memcached反射攻击的情况。 memcached反射攻击利用了在互联网上暴露的大批量memcached服务器（一种分布式缓存系统）存在的认证和设计缺陷，攻击者通过向memcached服务器IP地址的默认端口11211发送伪造受害者IP地址的特定指令UDP数据包（stats、set/get指令），使memcached服务器向受害者IP地址反射返回比原始数据包大数倍的数据（理论最高可达5万倍，通过持续跟踪观察攻击流量平均放大倍数在100倍左右），从而进行反射攻击。

【漏洞影响】

该项安全漏洞可能会导致产品被针对性的恶意利用，被利用发动大规模反射攻击。

【H3C产品】

自memcached反射攻击漏洞发布以来，H3C研发团队迅速进行了分析，对H3C公司产品进行了自查，结果如下。

确认涉及的产品：

l H3Cloud OS

确认不涉及产品：

l 园区核心交换机产品

l 数据中心交换机产品

l 园区接入交换机

l 无线产品

l 高端路由器

l 中低端路由器产品

l 核心路由器产品

l VNF2000系列产品（VSR/VBRAS/vFW/vLB/vAC/vLNS）

l 业务软件产品

l CAS

l 云桌面、云学堂系列产品

l H3Cloud AE/CE/CMP/OC/教育云

l 分布式存储

l H3C服务器产品

l 业务软件产品

l NFV产品

l SDN（vSwitch，SDN Controller和License Server）

l SDN广域网产品（AD-WAN）

l 大数据软件

l 安全产品

【H3C产品解决方案】

自memcached反射攻击漏洞发布以来，H3C 研发团队第一时间跟进该漏洞的原理分析和修复措施研究，并已经确定通过升级版本的方式可以有效地修复该安全漏洞，目前H3C研发团队正在实验室对修复后的底层软件进行功能与性能遍历测试。

涉及的产品的解决方案：

l H3Cloud OS

2018年3月底发布修复漏洞的升级版本，版本号E1139。

【H3C产品规避方案】

自memcached反射攻击漏洞发布以来，建议的规避方案如下：

1） 在memcached服务器或者其上联的网络设备上配置防火墙策略，仅允许授权的业务IP地址访问memcached服务器，拦截非法的非法访问。

2） 建议企业在出入口对源端口或目的端口为11211的UDP流量进行限速、限流和阻断，对被利用发起memcached反射攻击的用户IP进行处理。

3） 对H3Cloud OS产品，请参考 “附件1：H3Cloud OS针对由memcached服务器实施反射DDoS攻击漏洞的解决方案”，实施规避方案。