关于防范 MemcachedDDoS 攻击的通知

重庆太极发〔2018〕406 号　　签发人：杨靖

各公司、厂：

根据计算机信息安全漏洞相关报道，近日利用 memcached（高性能分布式内存对象缓存系统）服务器实施反射 DDOS 攻击的事件呈大幅上升趋势，该类型服务器主要用于大型电商网站或高并发访问网站。

国家有关部门监测发现 memcached 反射攻击自 2 月 21 日开始在我国境内活跃，3 月 1 日的攻击流量已超过传统反射攻击 SSDP 和 NTP 的攻击流量。随着 memcached 反射攻击方式被黑客了解和掌握，预测近期将出现更多该类攻击事件。按照中央网信办以及涪陵区互联网信息办公室的统一要求，需各单位加强对所属或第三方等提供的 Memcached 服务进行风险排查（若不涉及可忽略）。对排查发现的问题，应采取必要的整改措施，确保不存在可被利用的 Memcached 服务器主机。各单位若遭受攻击，应立即启动预案进行处置并报集团公司备案。

附件：处置建议

重庆太极实业（集团）股份有限公司

2018 年 4 月 23 日

附件

处置建议

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.更改 memcached 服务的监听端口为 11211 之外的其他大端口，避免针对默认端口的恶意利用。

3.升级到最新的 memcached 软件版本，配置启用 SASL 认证等权限控制策略(在编译安装 memcached 程序时添加–enable–sasl 选项，并且在启动 memcached 服务程序时添加–S 参数，启用 SASL 认证机制以提升 memcached 的安全性)。

详见

https://mp.weixin.qq.com/s/o564thhyY2zg0X7lu7ZneQ