

## 知 什么是Teardrop攻击?

攻击防范 金山 2016-09-10 发表

Teardrop 攻击指同一个IP.ID的多个分片报文之间，offset字段存在重叠。

比如说IP分片报文的首片长度是 1000，则第2片的offset字段就必须是1000，如果出现小于1000的情况，相当于第二片IP分片报文和第一片IP分片在重组的时候会出现重叠部分，此时防火墙等安全设备就会上报Teardrop攻击。