预警编号：YJ-2017022

恒安嘉新

关于 RTP 协议实现存在信息泄露漏洞（RTP Bleed）

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 09 月 14 日

1 漏洞描述

近日，互联网爆出 RTP 信息泄露漏洞（发现者命名为“RTP Bleed”），攻击者利用漏洞在不需要中间人身份的情况下，实现伪造音频注入，盗取音视频流或劫持语音通信，构成信息泄露和拒绝服务风险。因 RTP 协议的实现涉及较为广泛的中间件或应用软件，有可能造成大规模的影响，故恒安嘉新第一时间发布预警公告。该漏洞危害程度为”高危”。

2 影响范围

该漏洞可直接影响或间接影响到基于 RTP 协议的产品供应商或服务提供商。目前确认受影响的产品如下：

Asterisk 14.4.0

TPproxy (tested 1.2.1-2ubuntu1 and RTPproxy 2.2.alpha.20160822 (git))

3 漏洞原理

RTP 实时传输协议（Real-time Transport Protocol）是一种标准网络传输协议，RTP 协议主要实现在互联网上传递音频和视频的标准数据包格式。RTP 协议通常和 RTP 控制协议（RTCP）以及音视频流应用协议(H.323、 SIP)一起使用，广泛应用于流媒体相关的通讯和娱乐（如：网络电话、视频会议、网络电视和基于网络的一键通业务）。

该漏洞原理不同于“HeartBleed”漏洞。HeartBleed 是因 OpenSSL 组件漏洞而泄露内存信息，RTPBleed 是由于 RTP 协议实现缺陷而导致 RTP 流数据包存在暴露风险。

RTP Bleed 漏洞和 RTP 协议的设计虽有关联，但主要还是存在于 RTP 代理（Proxy）的具体实现上。RTP 代理主要通过在两个或多个参与方之间代理 RTP 流来解决影响 RTC 系统的 NAT 限制，RTP 代理由于不能直接信任流数据中的 RTP IP 和端口信息，而是以“学习模式”检查传入的 RTP 流量但又不使用身份验证机制。这使得攻击者可以直接接收 RTP 流媒体数据，且不需要中间人攻击条件。除上述攻击可能外，由于 RTP 代理和 RTP 协议堆栈在实现上轻易接受、转发或处理来自任何源的 RTP 包，因此攻击者可以发送特定构造的 RTP 数据包，注入至 RTP 流中。以上这两种攻击机制有可能导致流媒体信息泄露、会话劫持修改和拒绝服务。例如：攻击者可以将监听正在进行的电话呼叫或音视频会议。

4 修复建议

目前还未有正式解决方案，可以采取如下临时解决方案进行防范：

1） 在各类产品和中间件中启用安全实时传输协议（SRTP），可以避免机密性和完整性受影响；

2） SRTP 可以与其他技术措施（例如使用静态 IPS、支持 ICE 和 STUN authentication 等）相结合，可以避免对攻击途径的暴露。如：WebRTC 通过强制使用 SRTP 协议，就未受到漏洞的影响。