关于安全部分产品大量日志上送信息中心可能导致设备运行异常问题的技术公告

Syslog日志 Flow日志 **王晗** 2022-03-23 发表

问题描述

公告类别	强制立即整改
整改完成期限	2022/9/23
操作要求	配置更改

【产品型号】

F100系列、F1000系列、F5000系列、SecBlade FW 系列中低端防火墙；

T1000系列、T5000系列、SecBlade IPS 系列入侵防御；

L100系列、L1000系列、L5000系列、SecBlade ADE 系列负载均衡。

【涉及版本】

所有Comware V7版本。

【问题描述】

当大量安全模块日志（安全策略日志、流日志、威胁日志等）上送设备信息中心时，可能导致设备运行异常，出现无法登录、转发异常、设备挂死、设备重启等故障。

原因分析

【原因分析】

当日志量大的情况下，可能导致控制核繁忙，内部进程通信异常，同时转发性能下降。

规避措施/解决方案

【解决方案】

1、开启各安全模块记录日志功能时，必须同步配置快速日志（customlog）将对应模块日志发送至日志主机；

2、严禁配置Flow日志输出到信息中心。