OpenSSL “SSL-Death-Alert” 拒绝服务漏洞

漏洞 聂骋 2021-05-24 发表

漏洞相关信息

漏洞编号： CVE-2016-8610

漏洞名称： OpenSSL “SSL-Death-Alert” 拒绝服务漏洞

产品型号及版本： comware 及i-ware

漏洞描述

OpenSSL是OpenSSL团队开发的一个开源的能够实现安全套接层（SSL v2/v3）和安全传输层（TLS v1）协议的通用加密库，它支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。

OpenSSL的SSL/TLS协议握手过程实现中存在拒绝服务漏洞。攻击者可通过在一个消息中打包大量未定义类型警告包利用该漏洞使服务或进程陷入循环，造成拒绝服务（内存或CPU资源耗尽）。以下版本受到影响：

OpenSSL 1.1.0，OpenSSL 1.0.2 – 1.0.2h，OpenSSL All 1.0.1，OpenSSL All 0.9.8。

漏洞解决方案

comware 及 i-ware平台都不涉及。