iMC&U-Center是否涉及漏洞NVE-01-2014-08081

PLAT 高洋 2021-12-31 发表

漏洞相关信息

漏洞编号： NVE-01-2014-08081

漏洞名称： OpenSSL 心血漏洞检测(Heartbleed)

产品型号及版本： iMC_1.0系列产品，U-Center1.0系列产品

漏洞描述

OpenSSL TLS心跳扩展协议的实现上存在边界错误漏洞，远程无需验证的攻击者可以利用此漏洞导致泄漏64K的内存到连接的客户端或服务器，造成敏感信息的泄露。仅OpenSSL的1.0.1及1.0.2-beta版本受到影响，包括：1.0.1f及1.0.2-beta1版本。 TLS心跳由一个特殊构造请求包组成，其中包括有效载荷（payload），通信的另一方将读取这个包并发送一个响应，其中包含同样的载荷。在处理心跳请求的代码中，载荷大小是从攻击者可控的包中读取的。由于OpenSSL并没有检查该载荷大小值，从而导致越界读，造成了敏感信息泄漏。泄漏的信息内容可能会包括加密的私钥和其他敏感信息例如用户名、口令等。

漏洞解决方案

iMC&U-Center1.0系列皆不涉及该漏洞，可参考漏洞报告进行漏洞修复，不影响iMC&U-Center1.0功能。