iMC&U-Center是否涉及漏洞CVE-2016-6304

PLAT 汤祺 2021-03-22 发表

漏洞相关信息

漏洞编号： CVE-2016-6304

漏洞名称： openssl漏洞

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

【漏洞详情】

OpenSSL OCSP 状态请求扩展存在严重漏洞，该漏洞令恶意客户端能耗尽服务器内存。利用该漏洞，能使默认配置的服务器在每次协议重商时分配一段 OCSP ids 内存， 不断重复协商可令服务器内存无限消耗，即使服务器并未配置 OCSP。理论上，一个 OCSP id 最多 65,535 字节，攻击者可以不断重商令服务器每次内存消耗近 64K。但从实现来说，在 OpenSSL 1.0.2 版本中对 ClientHello 长度做了 16,384 字节的限制，因此每次重商只能令服务器内存消耗约 16K。但在最新的 1.1.0 版本中，对 ClientHello 长度的限制增加到 131,396 字节，那么对使用 1.1.0 版本的服务器，每次重商会令内存消耗近 64K。

【受影响版本】

iMC_PLAT_E0504P04以前版本

漏洞解决方案

iMC：升级平台至E0504P04及以上版本进行漏洞修复，组件版本需查看版本说明书中平台版本的适配关系确认是否需要同步升级

U-Center：不涉及