iMC&U-Center是否涉及漏洞CVE-2015-4000

PLAT 马永鸿 2022-10-24 发表

漏洞相关信息

漏洞编号： CVE-2015-4000
漏洞名称： TLS protocol中间人攻击漏洞
产品型号及版本： iMC/U-Center v7

漏洞描述

TLS（Transport Layer Security，安全传输层协议）是一套用于在两个通信应用程序之间提供保密性和数据完整性的协议。 TLS协议1.2及之前版本中存在安全漏洞。当服务器启用DHE_EXPORT密码套件时，程序未能正确传递DHE_EXPORT选项。攻击者可通过重写ClientHello（使用DHE_EXPORT取代DHE），然后重写ServerHello（使用DHE取代DHE_EXPORT），利用该漏洞实施中间人攻击和cipher-downgrade攻击。

漏洞解决方案

升级平台至E0708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