iMC&U-Center是否涉及漏洞CVE-2013-2566

PLAT 汤祺 2021-03-22 发表

漏洞相关信息

漏洞编号： CVE-2013-2566

漏洞名称： SSL/TLS RC4 信息泄露漏洞

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】

TLS协议和SSL协议中使用的的RC4算法中存在漏洞，该漏洞源于使用大量的单字节偏差。通过在使用相同明文的大量会话中密文的统计分析，远程攻击者利用该漏洞进行明文恢复攻击。

【受影响版本】

iMC_PLAT_E0403P10以前版本

漏洞解决方案

iMC：升级平台至E0403P10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