iMC&U-Center是否涉及漏洞CVE-2016-2183

PLAT 汤祺 2021-04-08 发表

漏洞相关信息

漏洞编号： CVE-2016-2183
漏洞名称： 检测到目标服务支持SSL中等强度加密算法
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】
SSL/TLS协议信息泄露漏洞(CVE-2016-2183)
TLS是安全传输层协议，用于在两个通信应用程序之间提供保密性和数据完整性。
TLS, SSH, IPSec协商及其他产品中使用的DES及Triple DES密码存在大约四十亿块的生日界，这可使远程攻击者通过Sweet32攻击，获取纯文本数据。
【受影响版本】
iMC_PLAT_0706以前版本

【漏洞扫描端口】
TCP 8443

漏洞解决方案

iMC：升级平台至E0706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：升级平台至E0706及以上版本进行漏洞修复，U-Center运维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