iMC&U-Center是否涉及漏洞CVE-2016-2178

PLAT 汤祺 2021-03-22 发表

漏洞相关信息

漏洞编号： CVE-2016-2178

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是一种开放源码的SSL实现，用来实现网络通信的高强度加密，现在被广泛地用于各种网络应用程序中。

OpenSSL <= 1.0.2h版本，crypto/dsa/dsa_ossl.c/dsa_sign_setup函数未正确使用恒时操作，本地用户通过定时旁侧攻击，可获取DSA密钥。

【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