iMC&U-Center是否涉及漏洞CVE-2014-3566

PLAT 汤祺 2021-03-22 发表

漏洞相关信息

漏洞编号： CVE-2014-3566

漏洞名称： SSL 3.0 POODLE攻击信息泄露漏洞

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】

为了通用性的考虑，目前多数浏览器版本都支持SSL3.0，TLS协议的握手阶段包含了版本协商步骤，一般来说，客户端和服务器端的最新的协议版本将会被使用。其在与服务器端的握手阶段进行版本协商的时，首先提供其所支持协议的最新版本，若该握手失败，则尝试以较旧的协议版本协商。能够实施中间人攻击的攻击者通过使受影响版本浏览器与服务器端使用较新协议的协商的连接失败，可以成功实现降级攻击，从而使得客户端与服务器端使用不安全的SSL3.0进行通信，此时，由于SSL 3.0使用的CBC块加密的实现存在漏洞，攻击者可以成功破解SSL连接的加密信息，比如获取用户COOKIE数据。这种攻击被称为POODL攻击(Padding Oracle On Downgraded Legacy Encryption)。

【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