iMC&U-Center是否涉及漏洞瞬时Diffie-Hellman 公共密钥过弱

PLAT 张兴龙 2022-09-27 发表

漏洞相关信息

漏洞编号： 无

漏洞名称： 瞬时 Diffie-Hellman 公共密钥过弱

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】

安全套接层（Secure Sockets Layer，SSL），一种安全协议，是网景公司（Netscape）在推出Web浏览器首版的同时提出的，目的是为网络通信提供安全及数据完整性。SSL在传输层对网络连接进行加密。传输层安全TLS（Transport Layer Security），IETF对SSL协议标准化（RFC 2246）后的产物，与SSL 3.0差异很小。

当服务器SSL/TLS的瞬时Diffie-Hellman公共密钥小于等于1024位时，存在可以恢复纯文本信息的风险。

【受影响版本】

iMC_PLAT_0706以前版本

【漏洞扫描端口】

8443

漏洞解决方案

升级到PLAT E0706版本后，找到iMC如下路径文件，备份后，使用附件文件替换下，替换完重启jserver进程 ，然后再扫描漏洞看下

$ iMC\client\conf\server.xml

附件下载：server.rar