技术公告号	KB0008390
发布日期	2025/11/07
文档版本(修订)	REV 1
适用产品名称	☒司印云打印 ☒司印涉密版
适用产品版本	V2.7.0.0/V3.0.0.0/V3.1.0.0/V3.2.0.0/V3.3.0.0

KB0008390- Apache Tomcat 相关漏洞对司印的影响

问题描述

CVE-2025-55752

该漏洞可能允许攻击者绕过访问控制，在某些配置下通过 HTTP PUT 请求上传恶意文件，进而导致潜在的远程代码执行。但 Apache 强调标准配置下利用可能性较低，因为"PUT 请求通常仅限于受信任用户，且不太可能同时启用 PUT 请求和 URI 操纵重写规则"。

影响范围
Tomcat 11.0.0-M1 至 11.0.10
Tomcat 10.1.0-M1 至 10.1.44
Tomcat 9.0.0.M11 至 9.0.108

漏洞利用条件：
1. 开启 put 指令
2. 开启 url 重写功能（配置 RewriteValve）
对司印影响： 司印服务器禁止 put 指令，也未开启 RewriteValve 功能，因此不受影响。

CVE-2025-55754

该漏洞影响运行在支持 ANSI 转义序列的 Windows 控制台环境中的 Tomcat 实例。公告解释称："Tomcat 未对日志消息中的 ANSI 转义序列进行转义处理。若 Tomcat 运行于 Windows 操作系统的控制台中，且该控制台支持 ANSI 转义序列，攻击者可能通过特制 URL 注入 ANSI 转义序列来操纵控制台和剪贴板，诱骗管理员执行攻击者控制的命令。"

影响范围
Tomcat 11.0.0-M1 至 11.0.10

Tomcat 10.1.0-M1 至 10.1.44
Tomcat 9.0.0.40 至 9.0.108

漏洞利用条件：
1. 将司印运行在控制台下
2. 控制台支持 ANSI 转义序列
对司印影响： 司印不以控制台运行，也不会将 url 信息写入控制台，因此不受影响。

CVE-2025-61795

该漏洞可能导致多文件上传期间出现拒绝服务（DoS）情况。当发生错误（如超过文件大小限制）时，上传文件的临时副本可能不会立即删除。Apache 说明："写入本地存储的上传部分临时副本未被立即清理，而是留待垃圾回收进程删除。根据 JVM 设置、应用程序内存使用情况和负载情况，临时副本占用的空间可能比 GC 清理速度更快地被填满，从而导致 DoS。"

影响范围：
Tomcat 11.0.0-M1 至 11.0.11
Tomcat 10.1.0-M1 至 10.1.46
Tomcat 9.0.0.M1 至 9.0.109

漏洞利用条件：
1. 多文件上传带来的 Dos 攻击
对司印影响：司印不支持多文件上传，因此不受影响。

解决方法

以上三个安全漏洞，虽然 Apache Tomcat 版本在影响范围内，但是由于司印不满足漏洞利用条件，因此对司印无影响，客户无需修复。
另外提供了补丁包，可将 Tomcat 版本升级至 9.0.111 或者 10.1.48，如有需要可下载升级。

司印服务器操作系统	补丁下载链接
Windows	https://console.box.lenovo.com/l/AogDZY 提取码：ezas
信创 X86	https://console.box.lenovo.com/l/EnyhED 提取码：jpmy
信创 ARM	https://console.box.lenovo.com/l/x1dSUh 提取码：vpbx