网络安全预警通报

2023 年第 4 期 （总第 41 期）

西安交通大学网络信息中心 2023 年 11 月 17 日

【预警类型】 **高危预警**

【预警内容】

关于海康威视部分综合安防管理平台产品存在任意文件上传漏洞

一、漏洞概述

海康威视部分综合安防管理平台历史版本由于对上传文件接口校验不足，攻击者可以将恶意文件上传到平台，导致获取服务权限或服务异常。

二、漏洞详情

海康威视运行管理中心前台存在命令执行漏洞利用详情：运行管理中心：/svm/api/v1/productFile 接口，仅对 token 有效性进行校验，利用 /iac/configService/v1/address 接口中泄漏的 token 即可对该接口进行未授权访问。

/svm/api/v1/productFil 接口可上传的压缩包，对压缩包文件的解压命令直接拼接了用户传入的 filename 参数导致远程命令执行

漏洞影响范围：

受影响的平台	受影响版本号
iVMS-8700	V2.0.0-V2.9.2
iSecure Center	V1.0.0-V1.7.0

三、处置建议

升级到系统版本的最新版本，如升级失败可联系海康客服获取帮助，详细修复方案请联系海康威视当地技术支持。

参考链接：

https://www.hikvision.com/cn/support/CybersecurityCenter/SecurityNotices/2023-03/