河南省教育信息安全监测中心

TellYouThePass 勒索事件

安全风险预警

河南省教育信息安全监测中心
Henan Provincial Education Information Security Monitoring Center

2023 年 11 月 23 日

TellYouThePass 勒索事件

安全风险预警

事件描述

针对近期发生的海康威视综合安防管理平台勒索攻击事件，攻击者利用历史已知的文件上传漏洞上传 Webshell 获取系统权限，并执行勒索病毒对文件进行加密，加密文件后缀为 locked1，同时生成勒索信息文件 README2.html。

locked1 病毒是 TellYouThePass 勒索家族变种之一，该家族主要通过已公开的 Nday 或未公开的 0day 漏洞进行大规模的无差别攻击。此外，TellYouThePass 是一个使用 Golang 语言编写的跨平台勒索病毒，支持对 Windows 及 linux 系统文件进行加密，由于使用了 RSA 非对称加密算法，目前尚无公开的解密密钥或解密方案。

漏洞编号

无

漏洞危害

高危

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

攻击排查

勒索事件涉及的漏洞为文件上传漏洞，该漏洞由于上传文件接口存在校验缺陷，导致攻击者可通过上传文件获取 Webshell 权限，并实现任意命令执行。

1、通过工具或命令行方式，排查综合安防管理平台相关 web 目录下是否存在异常 jsp 或 jspx 脚本文件。

windows 平台 web 目录路径如：

D:\hikvision\web\opsMgrCenter\bin\tomcat\apache-tomcat\webapps\clusterMgr。

Linux 平台 web 目录路径如：/opt/hikvision/web/components/tomcat85linux64.1/webapps/els/static 或 /opt/opsmgr/web/components/tomcat85linux64.1/webapps/els/static/

2、由于该平台默认并未启用 web 访问日志，导致无法通过日志对攻击行为进行分析，如存在第三方的日志平台，可检索相关上传接口是否存在异常请求，如：①/center/api/files;.js②/center/api/files;.html③/center/api/files;.png 等。

此外，通过平台报错日志@bic.center.error.log，可排查是否存在漏洞利用痕迹，windows 平台日志文件路径如：D:/hikvision/web/opsMgrCenter/logs/opsmgr_center。

安全建议

1、海康威视已于 2023 年 6 月发布了关于文件上传漏洞的安全通告并提供了修复方案，参考链接如下：

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

检查是否存在海康威视综合安防管理平台，并根据上述官方漏洞通告，及时更新平台版本修复漏洞。

2、关闭海康威视综合安防管理平台公网映射。

3、海康威视综合安防管理平台历史上还存在多个漏洞且在互联网公开，建议平台用户识别并且修复历史漏洞，避免因其他历史漏洞再次被攻击。

4、对综合安防管理平台进行必要的安全加固，包括降权平台运行账户，以防止攻击者利用 web 漏洞直接获取主机控制权限；启用 web 访问日志，以在事后对漏洞利用及攻击行为进行分析溯源等。

5、面对勒索攻击，在做好安全防护的同时，数据备份是最行之有效的对抗方案，可通过私有云、存储设备、网络同步等方式，定期对重要业务数据进行备份并妥善保管。

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893、0371-67765016

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052