09 任意视频删除漏洞

漏洞名称：任意视频删除漏洞
漏洞类别：横向越权
危害等级：严重
漏洞赏金：/
漏洞触发点：视频管理处
漏洞细节简述：审计JS代码视频删除函数，存在校验缺陷，可修改ID越权删除任意视频
参考来源：https://mp.weixin.qq.com/s/P_gYE85Jv7wE_TC3RojOGA
记录时间：2023.11.10

如何发现该漏洞?

- 下载 JS 代码审计分析，发现删除接口

如何审计JS代码?

- 通过接口定位到接口的函数
- 分析删除接口函数逻辑，发现没有权限校验
- 根据代码构造数据包测试

```
// 接口：/v1/videos/<video_id>/cta
export function updateCTA(videoId: string, ctaURL: string,
ctaText: string) {
    return getResults(
        appendQuery(`${TARGET_API_URL}videos/${video_id}/cta`, {
            api_key: WEB_API_KEY,
            link: ctaURL,
            text: ctaText,
        }),
        {
            method: ctaText ? 'put' : 'delete',
        }
    )
}
```