D2-10大华-智慧园区综合管理平台-文件上传

漏洞描述:

大华智慧园区综合管理平台 /emap/webservice/gis/soap/bitmap接口处存在任意文件上传漏洞,未授权的攻击者可以上传后门文件,执行任意命令,从而控制服务器权限。

网站图片:



建议使用谷歌浏览器,不支持IE浏览器

网络测绘:

fofa语法:

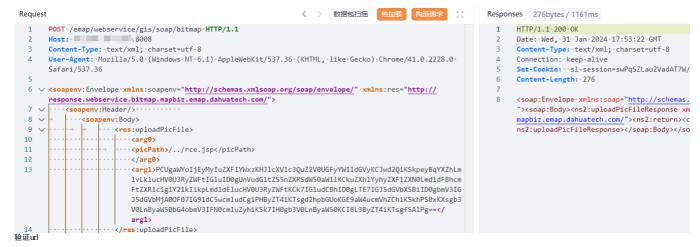
FOFA: app="dahua-智慧园区综合管理平台"

漏洞复现:

payload:

效果图:

PS:标签处为base64编码的马子



/upload/rce.jsp

RCE



uid=0(root) gid=0(root) groups=0(root)