Acunetix
by Invicti

# Affected Items Report

Acunetix Security Audit

2023-12-26

Generated by Acunetix

# Target - https://im.maixincloud.com/

## Scan details

| Scan information | |
|---|---|
| Start url | https://im.maixincloud.com/ |
| Host | https://im.maixincloud.com/ |

### Threat level

#### Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

### Alerts distribution

| | |
|---|---|
| Total alerts found | 17 |
| High | 1 |
| Medium | 10 |
| Low | 3 |
| Informational | 3 |

## Affected items

| Web Server | |
|---|---|
| **Alert group** | **~~TLS 1.0 已启用~~** |
| Severity | High |
| Description | 此 Web 服务器支持通过 TLS 1.0 加密。TLS 1.0 不被认为是“强密码术”。根据 PCI 数据安全标准 3.2(.1) 的定义和要求，在保护从网站往返的敏感信息时，TLS 1.0 并不被认为是 "强加密"。根据 PCI，"2018 年 6 月 30 日是禁用 SSL/早前 TLS 并实施更安全的加密协议 TLS 1.1 或更高版本（强烈建议 TLS v1.2）的最后期限，以便满足 PCI 数据安全标准 (PCI DSS)，保障支付数据的安全。 |
| Recommendations | 建议禁用 TLS 1.0 并替换为 TLS 1.2 或更高版本。 |
| Alert variants | |
| Details | The SSL server (port: 443) encrypts traffic using TLSv1.0. |

| Web Server | |
|---|---|
| **Alert group** | **~~CORS（跨域资源共享）来源验证失败~~** |
| Severity | Medium |
| Description | CORS（跨域资源共享）定义了一种允许客户端跨域请求的机制。此应用程序正以不安全的方式使用 CORS。<br><br>Web 应用程序无法正确验证来源报头（请查看“详细信息”部分以获取更多信息）并返回报头 **Access-Control-Allow-Credentials: true。**<br><br>在此配置中，任何网站均可发出通过**用户凭据**提出的请求并读取对这些请求的响应。信任任意来源会有效地禁用同源策略，从而允许第三方网站进行双向交互。 |
| Recommendations | 在 Access-Control-Allow-Origin 报头中仅允许选定的受信任域。 |
| Alert variants | |
| Details | Access-Control-Allow-Origin: **https://www.example.com**<br>Access-Control-Allow-Credentials: **true Any origin is accepted (arbitrary Origin header values are reflected in Access-Control-Allow-Origin response headers).** |

```
GET / HTTP/1.1

Origin: https://www.example.com

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36

Host: im.maixincloud.com

Connection: Keep-alive
```

| /css/ | |
|---|---|
| **Alert group** | **CORS（跨域资源共享）来源验证失败** |

| | |
|---|---|
| Severity | Medium |
| Description | CORS（跨域资源共享）定义了一种允许客户端跨域请求的机制。此应用程序正以不安全的方式使用 CORS。<br><br>Web 应用程序无法正确验证来源报头（请查看“详细信息”部分以获取更多信息）并返回报头 **Access-Control-Allow-Credentials: true。**<br><br>在此配置中，任何网站均可发出通过**用户凭据**提出的请求并读取对这些请求的响应。信任任意来源会有效地禁用同源策略，从而允许第三方网站进行双向交互。 |
| Recommendations | 在 Access-Control-Allow-Origin 报头中仅允许选定的受信任域。 |
| Alert variants | |
| Details | Access-Control-Allow-Origin: **https://www.example.com**<br>Access-Control-Allow-Credentials: **true Any origin is accepted (arbitrary Origin header values are reflected in Access-Control-Allow-Origin response headers).** |

```
GET /css/ HTTP/1.1

Origin: https://www.example.com

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36

Host: im.maixincloud.com

Connection: Keep-alive
```

| **/images/** | |
|---|---|
| **Alert group** | **CORS（跨域资源共享）来源验证失败** |
| Severity | Medium |
| Description | CORS（跨域资源共享）定义了一种允许客户端跨域请求的机制。此应用程序正以不安全的方式使用 CORS。<br><br>Web 应用程序无法正确验证来源报头（请查看“详细信息”部分以获取更多信息）并返回报头 **Access-Control-Allow-Credentials: true。**<br><br>在此配置中，任何网站均可发出通过**用户凭据**提出的请求并读取对这些请求的响应。信任任意来源会有效地禁用同源策略，从而允许第三方网站进行双向交互。 |
| Recommendations | 在 Access-Control-Allow-Origin 报头中仅允许选定的受信任域。 |
| Alert variants | |
| Details | Access-Control-Allow-Origin: **https://www.example.com**<br>Access-Control-Allow-Credentials: **true Any origin is accepted (arbitrary Origin header values are reflected in Access-Control-Allow-Origin response headers).** |

```
GET /images/ HTTP/1.1

Origin: https://www.example.com

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36

Host: im.maixincloud.com

Connection: Keep-alive
```

| **/IMFile/** | |
|---|---|
| **Alert group** | **CORS（跨域资源共享）来源验证失败** |
| Severity | Medium |
| Description | CORS（跨域资源共享）定义了一种允许客户端跨域请求的机制。此应用程序正以不安全的方式使用 CORS。<br><br>Web 应用程序无法正确验证来源报头（请查看“详细信息”部分以获取更多信息）并返回报头 **Access-Control-Allow-Credentials: true**。<br><br>在此配置中，任何网站均可发出通过**用户凭据**提出的请求并读取对这些请求的响应。信任任意来源会有效地禁用同源策略，从而允许第三方网站进行双向交互。 |
| Recommendations | 在 Access-Control-Allow-Origin 报头中仅允许选定的受信任域。 |
| Alert variants | |
| Details | Access-Control-Allow-Origin: **https://www.example.com**<br>Access-Control-Allow-Credentials: **true Any origin is accepted (arbitrary Origin header values are reflected in Access-Control-Allow-Origin response headers).** |

```
GET /IMFile/ HTTP/1.1

Origin: https://www.example.com

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36

Host: im.maixincloud.com

Connection: Keep-alive
```

| **/js/** | |
|---|---|
| **Alert group** | **CORS（跨域资源共享）来源验证失败** |
| Severity | Medium |

| | |
|---|---|
| Description | CORS（跨域资源共享）定义了一种允许客户端跨域请求的机制。此应用程序正以不安全的方式使用 CORS。<br><br>Web 应用程序无法正确验证来源报头（请查看“详细信息”部分以获取更多信息）并返回报头 **Access-Control-Allow-Credentials: true**。<br><br>在此配置中，任何网站均可发出通过**用户凭据**提出的请求并读取对这些请求的响应。信任任意来源会有效地禁用同源策略，从而允许第三方网站进行双向交互。 |
| Recommendations | 在 Access-Control-Allow-Origin 报头中仅允许选定的受信任域。 |
| Alert variants | |
| Details | Access-Control-Allow-Origin: **https://www.example.com**<br>Access-Control-Allow-Credentials: **true Any origin is accepted (arbitrary Origin header values are reflected in Access-Control-Allow-Origin response headers).** |

```
GET /js/ HTTP/1.1

Origin: https://www.example.com

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36

Host: im.maixincloud.com

Connection: Keep-alive
```

| **/lib/** | |
|---|---|
| **Alert group** | **CORS（跨域资源共享）来源验证失败** |
| Severity | Medium |
| Description | CORS（跨域资源共享）定义了一种允许客户端跨域请求的机制。此应用程序正以不安全的方式使用 CORS。<br><br>Web 应用程序无法正确验证来源报头（请查看“详细信息”部分以获取更多信息）并返回报头 **Access-Control-Allow-Credentials: true**。<br><br>在此配置中，任何网站均可发出通过**用户凭据**提出的请求并读取对这些请求的响应。信任任意来源会有效地禁用同源策略，从而允许第三方网站进行双向交互。 |
| Recommendations | 在 Access-Control-Allow-Origin 报头中仅允许选定的受信任域。 |
| Alert variants | |
| Details | Access-Control-Allow-Origin: **https://www.example.com**<br>Access-Control-Allow-Credentials: **true Any origin is accepted (arbitrary Origin header values are reflected in Access-Control-Allow-Origin response headers).** |

```
GET /lib/ HTTP/1.1

Origin: https://www.example.com

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36

Host: im.maixincloud.com

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **~~TLS 1.1 已启用~~** |
| Severity | Medium |
| Description | 此 Web 服务器支持通过 TLS 1.1 加密。当目标是支付卡行业 (PCI) 数据安全标准 (DSS) 合规性时，建议（尽管在当时或书面上并不需要）使用 TLS 1.2 或更高版本。根据 PCI，"2018 年 6 月 30 日是禁用 SSL/早前 TLS 并实施更安全的加密协议 TLS 1.1 或更高版本（强烈建议 TLS v1.2）的最后期限，以便满足 PCI 数据安全标准 (PCI DSS)，保障支付数据的安全。 |
| Recommendations | 建议禁用 TLS 1.1 并替换为 TLS 1.2 或更高版本。 |
| Alert variants | |
| Details | The SSL server (port: 443) encrypts traffic using TLSv1.1. |

| **Web Server** | |
|---|---|
| **Alert group** | **~~TLS/SSL LOGJAM 攻击~~** |
| Severity | Medium |
| Description | LOGJAM 攻击是一个 SSL/TLS 漏洞，允许攻击者拦截易受攻击的客户端和服务器之间的 HTTPS 连接，并强制它们使用“导出级”加密，然后可以对其进行解密或更改。发现网站支持 DH(E) 导出密码套件，或使用小于 1024 位的 DH 素数或最大 1024 位的常用 DH 标准素数的非导出 DHE 密码套件时，会发出此漏洞警报。 |
| Recommendations | 重新配置受影响的 SSL/TLS 服务器以禁用对任何 DHE_EXPORT 套件的支持，DH 素数需小于 1024 位，DH 标准素数最大为 1024 位。请参阅《适用于 TLS 的Diffie-Hellman 部署指南》，获取有关如何相应部署受影响系统的进一步指导。 |
| Alert variants | |

| | |
|---|---|
| Details | Weak DH Key Parameters (p < 1024 bits, or <= 1024 bits for common primes):<br><br>• TLS1.0, TLS_DHE_RSA_WITH_AES_256_CBC_SHA: 1024 bits (common prime)<br>• TLS1.0, TLS_DHE_RSA_WITH_AES_128_CBC_SHA: 1024 bits (common prime)<br>• TLS1.1, TLS_DHE_RSA_WITH_AES_256_CBC_SHA: 1024 bits (common prime)<br>• TLS1.1, TLS_DHE_RSA_WITH_AES_128_CBC_SHA: 1024 bits (common prime)<br>• TLS1.2, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384: 1024 bits (common prime)<br>• TLS1.2, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256: 1024 bits (common prime)<br>• TLS1.2, TLS_DHE_RSA_WITH_AES_256_CBC_SHA: 1024 bits (common prime)<br>• TLS1.2, TLS_DHE_RSA_WITH_AES_128_CBC_SHA: 1024 bits (common prime) |

| **Web Server** | |
|---|---|
| **Alert group** | **~~TLS/SSL Sweet32 攻击~~** |
| Severity | Medium |
| Description | Sweet32 攻击是一个 SSL/TLS 漏洞，允许攻击者使用 64 位分组密码破坏 HTTPS 连接。 |
| Recommendations | 重新配置受影响的 SSL/TLS 服务器以禁用对废弃 64 位分组密码的支持。 |
| Alert variants | |
| Details | Cipher suites susceptible to Sweet32 attack (TLS1.0 on port 443):<br><br>• TLS_RSA_WITH_3DES_EDE_CBC_SHA<br><br>Cipher suites susceptible to Sweet32 attack (TLS1.1 on port 443):<br><br>• TLS_RSA_WITH_3DES_EDE_CBC_SHA<br><br>Cipher suites susceptible to Sweet32 attack (TLS1.2 on port 443):<br><br>• TLS_RSA_WITH_3DES_EDE_CBC_SHA |

| **Web Server** | |
|---|---|
| **Alert group** | **~~TLS/SSL 弱密码套件~~** |
| Severity | Medium |
| Description | 远程主机支持带弱或不安全属性的 TLS/SSL 密码套件。 |
| Recommendations | 重新配置受影响的应用程序以避免使用弱密码套件。 |
| Alert variants | |

| | |
|---|---|
| Details | Weak TLS/SSL Cipher Suites: (offered via TLS1.0 on port 443):<br><br>• TLS_RSA_WITH_3DES_EDE_CBC_SHA (Medium strength encryption algorithm (3DES).)<br>• TLS_RSA_WITH_RC4_128_SHA (Weak encryption algorithm (RC4).)<br>• TLS_RSA_WITH_RC4_128_MD5 (Weak encryption algorithm (RC4). MD5-HMAC.)<br><br>Weak TLS/SSL Cipher Suites: (offered via TLS1.1 on port 443):<br><br>• TLS_RSA_WITH_3DES_EDE_CBC_SHA (Medium strength encryption algorithm (3DES).)<br>• TLS_RSA_WITH_RC4_128_SHA (Weak encryption algorithm (RC4).)<br>• TLS_RSA_WITH_RC4_128_MD5 (Weak encryption algorithm (RC4). MD5-HMAC.)<br><br>Weak TLS/SSL Cipher Suites: (offered via TLS1.2 on port 443):<br><br>• TLS_RSA_WITH_3DES_EDE_CBC_SHA (Medium strength encryption algorithm (3DES).)<br>• TLS_RSA_WITH_RC4_128_SHA (Weak encryption algorithm (RC4).)<br>• TLS_RSA_WITH_RC4_128_MD5 (Weak encryption algorithm (RC4). MD5-HMAC.) |

| **Web Server** | |
|---|---|
| **Alert group** | **~~点击劫持：X-Frame-Options 报头缺失~~** |
| Severity | Low |
| Description | 点击劫持（用户界面矫正攻击、UI 矫正攻击、UI 矫正）是一种恶意技术，诱使 Web 用户点击与用户认为其单击的内容不同的内容，从而在单击看似无害的网页时有可能导致机密信息泄露或计算机被控制 。<br><br>服务器未返回 X-Frame-Options **报头，这意味着此网站存在遭受点击劫持攻击的风险。X-Frame-Options HTTP 响应报头可被用于指示是否应允许浏览器在框架或 iframe 内呈现页面。站点可以通过确保其内容中未嵌入其他网站来避免点击劫持攻击。** |
| Recommendations | 配置您的 Web 服务器，使其包含 X-Frame-Options 报头和带有 frame-ancestors 指令的 CSP 报头。有关该报头可能值的更多信息，请查阅 Web 参考资料。 |
| Alert variants | |
| Details | 不包含 XFO 报头的路径：<br><br>• https://im.maixincloud.com/<br>• https://im.maixincloud.com/images/<br>• https://im.maixincloud.com/css/<br>• https://im.maixincloud.com/IMFile/<br>• https://im.maixincloud.com/js/<br>• https://im.maixincloud.com/main<br>• https://im.maixincloud.com/lib/ |

```
GET / HTTP/1.1

Referer: https://im.maixincloud.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36

Host: im.maixincloud.com

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **~~可缓存敏感页面~~** |
| Severity | Low |
| Description | 一个或多个页面可能包含敏感信息（例如，密码参数），且可能被潜在缓存。即使在安全的 SSL 通道中，中介代理和 SSL 终接器也可以存储敏感数据。要防止这一点，应指定一个 Cache-Control 报头。 |
| Recommendations | 通过添加 "Cache Control: No-store" 和 "Pragma: no-cache" 至 HTTP 响应报头，阻止缓存。 |
| Alert variants | |
| Details | 可以缓存的页面列表：<br>• https://im.maixincloud.com/main?ErrMsg=Index%20was%20outside%20the%20bounds%20of%20the%20array.&UserName=<br>• https://im.maixincloud.com/main?ErrMsg=&UserName= |

```
GET /main?ErrMsg=Index%20was%20outside%20the%20bounds%20of%20the%20array.&UserName=
HTTP/1.1

Referer: https://im.maixincloud.com/Login

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36

Host: im.maixincloud.com

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | **~~未实施 HTTP 严格传输安全 (HSTS)~~** |
| Severity | Low |

| | |
|---|---|
| Description | HTTP 严格传输安全 (HSTS) 规定，浏览器只能使用 HTTPS 访问网站。检测到您的 Web 应用程序未实施 HTTP 严格传输安全 (HSTS)，因为响应中缺少严格传输安全报头。 |
| Recommendations | 建议在您的 Web 应用程序中实施 HTTP 严格传输安全 (HSTS)。请查询网络参考文件以了解更多信息 |
| Alert variants | |
| Details | 未启用 HSTS 的 URL：<br>• https://im.maixincloud.com/<br>• https://im.maixincloud.com/images/<br>• https://im.maixincloud.com/css/<br>• https://im.maixincloud.com/IMFile/<br>• https://im.maixincloud.com/js/<br>• https://im.maixincloud.com/main<br>• https://im.maixincloud.com/lib/ |

```
GET / HTTP/1.1

Referer: https://im.maixincloud.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36

Host: im.maixincloud.com

Connection: Keep-alive
```

| | |
|---|---|
| **Web Server** | |
| **Alert group** | **~~Microsoft IIS 版本披露~~** |
| Severity | Informational |
| Description | 此 Web 应用程序返回的 HTTP 响应包含一个名为 **Server** 的报头。此报头的值包含 Microsoft IIS 服务器的版本。 |
| Recommendations | Microsoft IIS 应被配置成从响应中移除不需要的 HTTP 响应报头。请查阅网络参考文献了解更多信息。 |
| Alert variants | |
| Details | 找到版本信息：<br>`Microsoft-IIS/8.5` |

```
GET /|~.aspx HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36

Host: im.maixincloud.com

Connection: Keep-alive
```

| **Web Server** | |
|---|---|
| **Alert group** | ~~**TLS/SSL (EC)DHE 密钥重用**~~ |
| Severity | Informational |
| Description | 远程主机重新使用带 (EC)DHE 密码套件的 Diffie-Hellman Ephemeral 公共服务器密钥。 |
| Recommendations | 重新配置受影响的应用程序，以在使用 tmp_dh/tmp_ecdh 参数时总是生成新密钥。 |
| Alert variants | |
| Details | Diffie-Hellman Public Key Reuse:<br><br>• ECDHE public server key reuse: 04 aa 9a 41 c2 4c e5 5c c4 95 8f b2 46 5b 51 16 3f 00 c4 f8 47 06 36 2b 65 e0 5f 3e 93 95 fe 63 fb 09 11 63 57 0c 46 ac e3 64 70 2f fd 3d 2b 1d 20 35 f5 d2 47 45 99 37 7f 5d 30 2d 3a 4f bf 0a 10 (with TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA) |

| **Web Server** | |
|---|---|
| **Alert group** | ~~**未实施内容安全策略 (CSP)**~~ |
| Severity | Informational |
| Description | 内容安全策略 (CSP) 增加了额外的安全层，有助于检测和缓解某些类型的攻击，包括跨站脚本 (XSS) 和数据注入攻击。<br><br>内容安全策略 (CSP) 可通过添加 **Content-Security-Policy** 报头实施。此报头的值是一个字符串，其中包含描述内容安全策略的策略指令。要实施 CSP，您应该为站点使用的所有资源类型定义允许的来源列表。例如，如果您有一个简单的站点，需要从 CDN 加载本地托管和 jQuery 库中的脚本、样式表和图像，则 CSP 报头可能如下所示：<br><br>`Content-Security-Policy: default-src 'self'; script-src 'self' http`<br><br>检测到您的 Web 应用程序未实施内容安全策略 (CSP)，因为响应中缺少 CSP 报头。建议在您的 Web 应用程序中实施内容安全策略 (CSP)。 |
| Recommendations | 建议在您的 Web 应用程序中实施内容安全策略 (CSP)。配置内容安全策略涉及添加 **Content-Security-Policy** HTTP 报头到 Web 页面并为其赋值，以控制允许用户代理为该页面加载的资源。 |
| Alert variants | |

| | |
|---|---|
| Details | 不包含 CSP 报头的路径：<br>• https://im.maixincloud.com/<br>• https://im.maixincloud.com/images/<br>• https://im.maixincloud.com/css/<br>• https://im.maixincloud.com/IMFile/<br>• https://im.maixincloud.com/js/<br>• https://im.maixincloud.com/main<br>• https://im.maixincloud.com/lib/ |

```
GET / HTTP/1.1

Referer: https://im.maixincloud.com/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/92.0.4512.0 Safari/537.36

Host: im.maixincloud.com

Connection: Keep-alive
```

## Scanned items (coverage report)

https://im.maixincloud.com/
https://im.maixincloud.com/css/
https://im.maixincloud.com/images/
https://im.maixincloud.com/IMFile/
https://im.maixincloud.com/js/
https://im.maixincloud.com/lib/