Burp Scanner Report

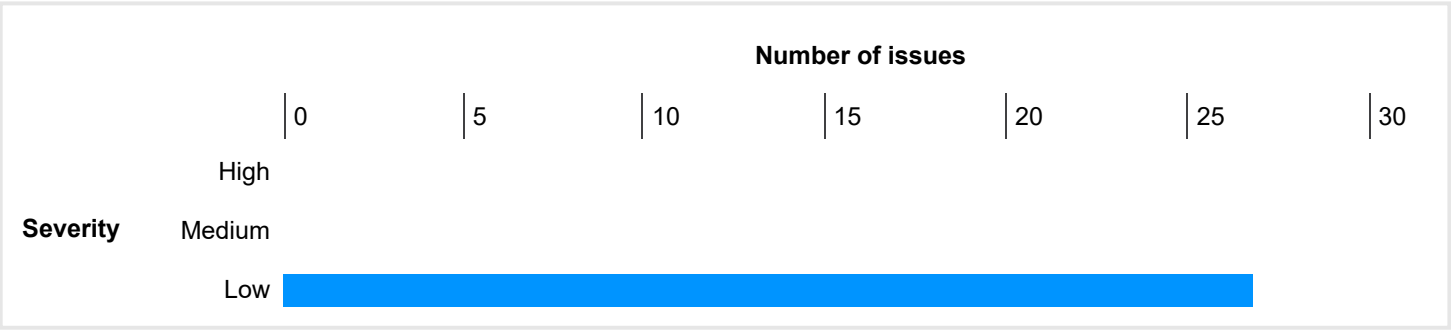
Burp Suite Professional

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low, Information or False Positive. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	0	0	0	0
	Medium	0	0	0	0
	Low	23	0	0	23
	Information	27	2	0	29
	False Positive	0	0	0	0

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1.10. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html
1.11. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js
1.12. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.appcache
1.13. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html
1.14. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.js
1.15. https://tnzslk-launches.appsflyersdk.com/api/v6.12/androidevent
1.16. https://www.deliverizate.es/
1.17. https://www.deliverizate.es/api/getUserInfo
1.18. https://www.deliverizate.es/api/saveImageF
1.19. https://www.deliverizate.es/api/signup
1.20. https://www.deliverizate.es/api/userNearByMePageFilters
1.21. https://www.deliverizate.es/storage/mainimage/1731198209IMG_20241109_162327800.jpg
1.22. https://www.deliverizate.es/storage/mainimage/1732858484premium_photo-1671656349322-41de944d259b.jpeg
1.23. https://www.deliverizate.es/storage/thumbnails/1731198209IMG_20241109_162327800.jpg

2. Cookie scoped to parent domain

3. Cross-domain Referer leakage

4. Frameable response (potential Clickjacking)

5. Browser cross-site scripting filter disabled

5.1. https://dl.google.com/vision/1/creditcard/gocr_credit_card_ocr_v0.zip
5.2. https://fonts.googleapis.com/css
5.3. https://fundingchoicesmessages.google.com/a/consent
5.4. https://googleads.g.doubleclick.net/
5.5. https://googleads.g.doubleclick.net/favicon.ico
5.6. https://googleads.g.doubleclick.net/getconfig/pubsetting
5.7. https://googleads.g.doubleclick.net/mads/gma
5.8. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html
5.9. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js
5.10. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.appcache
5.11. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html
5.12. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.js

6. Email addresses disclosed

6.1. https://googleads.g.doubleclick.net/mads/gma
6.2. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html
6.3. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js
6.4. https://www.deliverizate.es/api/userNearByMePageFilters

7. Cacheable HTTPS response

7.1. https://dl.google.com/vision/1/creditcard/gocr_credit_card_ocr_v0.zip
7.2. https://geomobileservices-pa.googleapis.com/google.internal.maps.geomobileservices.geocoding.v3mobile.GeocodingService/ReverseGeocode
7.3. https://gmscompliance-pa.googleapis.com/google.internal.gmscore.gmscompliance.v1.GmsCompliance/GetEnforcement
7.4. https://googleads.g.doubleclick.net/getconfig/pubsetting
7.5. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/native_ads.html
7.6. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html
7.7. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.appcache
7.8. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html

8. Base64-encoded data in parameter

9. Content type is not specified

1. Strict transport security not enforced

There are 23 instances of this issue:

- https://dl.google.com/vision/1/creditcard/gocr_credit_card_ocr_v0.zip
- https://fonts.googleapis.com/css
- https://fundingchoicesmessages.google.com/a/consent
- https://geomobileservices-pa.googleapis.com/google.internal.maps.geomobileservices.geocoding.v3mobile.GeocodingService/ReverseGeocode
- https://gmscompliance-pa.googleapis.com/google.internal.gmscore.gmscompliance.v1.GmsCompliance/GetEnforcement
- https://googleads.g.doubleclick.net/
- https://googleads.g.doubleclick.net/favicon.ico
- https://googleads.g.doubleclick.net/getconfig/pubsetting
- https://googleads.g.doubleclick.net/mads/gma
- https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html
- https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js
- https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.appcache
- https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html
- https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.js
- https://tnzslk-launches.appsflyersdk.com/api/v6.12/androidevent
- https://www.deliverizate.es/
- https://www.deliverizate.es/api/getUserInfo
- https://www.deliverizate.es/api/saveImageF
- https://www.deliverizate.es/api/signup
- https://www.deliverizate.es/api/userNearByMePageFilters
- https://www.deliverizate.es/storage/mainimage/1731198209IMG_20241109_162327800.jpg
- https://www.deliverizate.es/storage/mainimage/1732858484premium_photo-1671656349322-41de944d259b.jpeg
- https://www.deliverizate.es/storage/thumbnails/1731198209IMG_20241109_162327800.jpg

Issue description

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Issue remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

References

- HTTP Strict Transport Security
- sslstrip
- HSTS Preload Form

Vulnerability classifications

- CWE-523: Unprotected Transport of Credentials
- CAPEC-94: Man in the Middle Attack
- CAPEC-157: Sniffing Attacks

1.1. https://dl.google.com/vision/1/creditcard/gocr_credit_card_ocr_v0.zip

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://dl.google.com**
Path:	**/vision/1/creditcard/gocr_credit_card_ocr_v0.zip**

Request

```
GET /vision/1/creditcard/gocr_credit_card_ocr_v0.zip HTTP/2
Host: dl.google.com
User-Agent: com.google.android.gms/244534025 (Linux; U; Android 11; en_US; sdk_gphone_x86; Build/RSR1.201013.001; Cronet/132.0.6779.0)
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Disposition: attachment
Content-Security-Policy: default-src 'none'
Server: downloads
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 0
Date: Fri, 29 Nov 2024 05:35:31 GMT
Cache-Control: public,max-age=86400
Last-Modified: Fri, 21 Oct 2022 23:56:48 GMT
Etag: "fd7fee"
Content-Type: application/zip
Content-Length: 696543
Age: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

PK.....!()(x.....credit_card_ocr_engine.binarypb.T]k.A.e..uj?..b..].-E..M.m@..m.4M.)(.....]..Yfg.....D.....?A_|.._..n..h>...
{..s.=w.....].[...I...|A.^    8.....9/b..I.H..+;.....&-.f.!
...[SNIP]...
```

1.2. https://fonts.googleapis.com/css

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://fonts.googleapis.com**

Path: **/css**

Request

```
GET /css?family=System%20Font%20(Default)|System%20Font%20(Default)|System%20Font%20(Default) HTTP/2
Host: fonts.googleapis.com
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36
Accept: text/css,*/*;q=0.1
X-Requested-With: com.datingpro.dolly
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: style
Accept-Encoding: gzip, deflate, br
Accept-Language: en,en-US;q=0.9
```

Response

```
HTTP/2 400 Bad Request
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Mon, 01 Jan 1990 00:00:00 GMT
Date: Fri, 29 Nov 2024 05:33:35 GMT
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy: same-origin-allow-popups
Server: ESF
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

<!DOCTYPE html><html lang=en><head><meta charset=utf-8><title>400: Font family not found</title><link href="//fonts.googleapis.com/css?family=Open+Sans:300,400" rel="stylesheet" type="text/css"/><styl
...[SNIP]...
```

1.3. https://fundingchoicesmessages.google.com/a/consent

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://fundingchoicesmessages.google.com**

Path: **/a/consent**

Request

```
POST /a/consent HTTP/1.1
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36
Content-Type: application/json
Host: fundingchoicesmessages.google.com
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
Content-Length: 448

{"admob_app_id":"ca-app-pub-2489227358200851~5341356166","is_lat":false,"adid":"f20fbe71-dba0-4c12-8b2e-6cbbc3d4cdfe","device_info":{"os_type":"ANDROID","model":"sdk_gphone_x86","android_api_level":30
...[SNIP]...
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Mon, 01 Jan 1990 00:00:00 GMT
Date: Fri, 29 Nov 2024 05:35:02 GMT
Content-Disposition: attachment; filename="json.txt"; filename*=UTF-8"json.txt
Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/ContributorServingAppSwitchboardHttp/cspreport
Content-Security-Policy: script-src 'report-sample' 'nonce-v2wT9LASY56K_F2eueDIZg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/ContributorServingAppSwitchboardHttp/cspreport;worker-src 'self'
Content-Security-Policy: script-src 'unsafe-inline' 'unsafe-eval' blob: data: 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.googletagmanager.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/ContributorServingAppSwitchboardHttp/cspreport/allowlist
Accept-Ch: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-WoW64, Sec-CH-UA-Form-Factors, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version
Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-wow64=*, ch-ua-form-factors=*, ch-ua-platform=*, ch-ua-platform-version=*
Cross-Origin-Opener-Policy: same-origin
Reporting-Endpoints: default="/_/ContributorServingAppSwitchboardHttp/web-reports?context=eJzjStDikmLw1pBikPj6kkkDiJ3SZ7AGAXHrzXOsU4E46d951iIgNlS4xOoIwkWXWD2BWLXnEqspEN9fd4n1ORDPOH-ZdQEQF0lcYW0CYoavV1g5gFiIh6Nt6dJdbAI3bi18zaikkZRfGJ-cn1dSlJlUWpJflJacllqcWlSWWhRvZGBkYmhoaKlnYBhfYAAA4Gs9jw"
Server: ESF
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

)]}'
{
"consent_signal": "CONSENT_SIGNAL_NOT_REQUIRED",
"consent_form_base_url": "about:blank/",
"request_info_keys": ["IABTCF_TCString", "IABTCF_AddtlConsent", "IABTCF_idfaFlowControl", "IDFA_f
...[SNIP]...
```

1.4. https://geomobileservices-pa.googleapis.com/google.internal.maps.geomobileservices.geocoding.v3mobile.GeocodingService/ReverseGeocode

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://geomobileservices-pa.googleapis.com**
Path:	**/google.internal.maps.geomobileservices.geocoding.v3mobile.GeocodingService/ReverseGeocode**

Request

```
POST /google.internal.maps.geomobileservices.geocoding.v3mobile.GeocodingService/ReverseGeocode HTTP/1.1
Host: geomobileservices-pa.googleapis.com
User-Agent: com.google.android.gms/244534025 (Linux; U; Android 11; en_US; sdk_gphone_x86; Build/RSR1.201013.001; Cronet/132.0.6779.0) grpc-java-cronet/1.69.0-SNAPSHOT
Content-Type: application/grpc
Te: trailers
X-Goog-Spatula: CjYKFmNvbS5nb29nbGUuYW5kcm9pZC5nbXMaHE9KR0tSVDBIR1pOVStMR2E4RjdHVml6dFY0Zz0Y8M6FupvDrb04
Grpc-Accept-Encoding: gzip
Grpc-Timeout: 9952874u
Content-Length: 52
Connection: keep-alive

..../
.    *}....B@..=..`.^...en0.:.com.datingpro.dolly
```

Response

```
HTTP/2 200 OK
Content-Disposition: attachment
Content-Type: application/grpc
Date: Fri, 29 Nov 2024 05:35:00 GMT
Server-Timing: gfet4t7; dur=29
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Grpc-Status: 0
Content-Disposition: attachment

.....
..
...FGoogle Building 43, 43 Amphitheatre Pkwy, Mountain View, CA 94043, USA.+
....Google Building 43..Google Building 43..
."..43..43.,
....Amphitheatre Parkway..Amphitheatre Pkwy."
....Mount
...[SNIP]...
```

1.5. https://gmscompliance-pa.googleapis.com/google.internal.gmscore.gmscompliance.v1.GmsCompliance/GetEnforcement

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://gmscompliance-pa.googleapis.com**
Path:	**/google.internal.gmscore.gmscompliance.v1.GmsCompliance/GetEnforcement**

Request

```
POST /google.internal.gmscore.gmscompliance.v1.GmsCompliance/GetEnforcement HTTP/2
Host: gmscompliance-pa.googleapis.com:443
User-Agent: grpc-java-okhttp/1.69.0-SNAPSHOT
Content-Type: application/grpc
Te: trailers
X-Goog-Api-Key: AIzaSyAP-gfH3qvi6vgHZbSYwQ_XHqV_mXHhzIk
X-Android-Package: com.google.android.gms
X-Android-Cert: 38918A453D07199354F8B19AF05EC6562CED5788
Grpc-Accept-Encoding: gzip
Grpc-Timeout: 59908669u
Content-Length: 8212

... .

.........8...
Rgoogle/sdk_gphone_x86/generic_x86_arm:11/RSR1.201013.001/6903271:user/release-
keys..google..sdk_gphone_x86".generic_x86_arm*.Google2.sdk_gphone_x86:.@.JRgoogle/sdk_gphone_x86/gen
...[SNIP]...
```

Response

```
HTTP/2 200 OK
Content-Type: application/grpc
Grpc-Accept-Encoding: identity, deflate, gzip
Content-Disposition: attachment
Date: Fri, 29 Nov 2024 05:33:35 GMT
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Grpc-Status: 0
Endpoint-Load-Metrics-Bin: MeTOEIDQIzBASY9MYzs/e9A/
Grpc-Server-Stats-Bin: AACx+bYCAAAAAA
Pc-High-Bwd-Bin: S2dJWUN3

....c
....................."
.........8*..
Rgoogle/sdk_gphone_x86/generic_x86_arm:11/RSR1.201013.001/6903271:user/release-
keys..google..sdk_gphone_x86".generic_x86_arm*.Google2.sdk_gphone_x86:.@.JRgoog
...[SNIP]...
```

1.6. https://googleads.g.doubleclick.net/

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/**

Issue detail

This issue was found in multiple locations under the reported path.

Request

GET /mads/gma?submodel=sdk_gphone_x86&adid_p=1&format=interstitial_mb&omid_v=a.1.4.14-google_20240908&client_purpose_one=false&dv=243799205&ev=22.1.0&hl=en&js=afma-sdk-a-v243799999.231004000.1&lv=231004600&ms=CpgECoACRfDsdkLgM3pvTf543jF5aNwK_FsZltWJnMebuy4VHmqQHgKu7q1cYr-w4lInWAHEpaY1de8DFoOYV0yxEqoIlkDpeM0n0pDXK6sh0vhr8IcVQnF6MG41wtF09YDNkSkS3ReAUnPsmFKeo_XkIVL4a2Bqv40YOeMt8YA27xb9w7gPb3MAFmMDTvv8ricGdZS5237j86jtGvqcuPhoQr1vBOJkq_-kABbYk1c2jXcO7Ixc5XlyAjcvH-Fwc0CW8UbEXvLBwSy_Fwr94iXQcUsxo0XI1eQNYC3rf3tUdHKAsHvxK3g2EhMTa3n8Jokw4Hg-7OtsxvH4AkMfkepJ9CEROgqAAouyqEZjTD1U-KRw7Vfq9kRX0yMhCulSOshe3oLgMwyi74fI_uXlaxM5DQnYPH20Lc3xG2stEpXxp4hdsJrrbD9m7Z0xnLWLwE8vsb6NMWS2Y3Uu6bh3I5AePj5DM4-snFuhzxzgG6MikOzCps7pjTswaIhn63xperuTq63DGn4JQc3z4iFLqJ-Gc77p1p-w5fG39Bq5J1W9854FVR2Vp35QX4RZiLtpPIRO7G5QJTosP8FxFXPLwmGxWsFQHZ6TJng1uBmloLBiS-Gudm35WXflOEFdj2q7G4FUeliqo0KynpLhq06HKYi5l3x4lWiWkZbWOyM2tPMLF_pOaRg7ZIQSEKI6D4fWKdQYbWUbG47ZKv4SlQIKgALwk4mbIQMYmOi1dxKEEjD9DBRpD9oyAu_oCkcknszXA-BeM1IXHawwLMtZ_90ltPfv6k81kaY78Nlo6oqglnBWDdSwDw0qA5lvhjvcHeoHOuKAS8JIVwfrs1e3OZQaaDc6ULU43qybe7AAAj0zBtG91pFH1sqlq-bjMLg0jKnHLYimrnwXBKKZUtKQI80qZNobipC4OKjFSkidzn_zufLiMIgJ9KOYxkBKcTZH9x7LE5am6oozeHiYntSmt345ajwa-8wF3K0VkVin7-_v31mF5ZDL5PEFH-18PZZElsBOlbiqFP7F1IbdDhCTpI9PlJKVH2pB5TTeyTQdDe7zKUyOEhA5DX8SsA0J-NjRzaSUuUmd&mv=84371920.com.android.vending&lft=0&vnm=3.5.7&risd=1&u_sd=2.625&request_id=202454318&target_api=34&carrier=310260&fbs_aeid=-6234431077831155455&fbs_aiid=e2f6cf45cddfbfd5703631a763303552&seq_num=1&eid=318502753%2C318515867%2C318516088%2C318516381%2C318516383&guci=0.0.0.0.0.0.0.0&adtest=on&sdk_apis=7%2C8&omid_p=Google%2Fafma-sdk-a-v243799999.231004000.1&u_w=412&u_h=684&msid=com.datingpro.dolly&an=102.android.com.datingpro.dolly&u_audio=4&net=wi&u_so=p&preqs_in_session=0&preqs=0&time_in_session=0&sst=1732858500000&output=html&region=mobile_app&u_tz=-300&client=ca-app-pub-2489227358200851&slotname=2809117006&gsb=wi&apm_app_id=1%3A20824395699%3Aandroid%3A9d3ef0a0146f0e1a6fc5c6&gmp_app_id=1%3A20824395699%3Aandroid%3A9d3ef0a0146f0e1a6fc5c6&apm_app_type=1&lite=0&num_ads=1&vpt=8&vfmt=18&vst=0&sdkv=o.243799999.231004000.1&sdmax=0&dmax=1&sdki=3c4d&stbg=1&caps=inlineVideo_interactiveVideo_mraid1_mraid2_mraid3_sdkVideo_exo3_th_autoplay_mediation_scroll_av_transparentBackground_sdkAdmobApiForAds_di_aso_sfv_dinm_dim_nav_navc_dinmo_ipdof_gls_xSeconds&bisch=false&blev=1&canm=false&_mv=84371920.com.android.vending&heap_free=8095765&heap_max=536870912&heap_total=25194957&wv_count=1&rdps=4250&is_lat=false&rdidl=36&idtypel=4&blob=ABPQqLGGVg2RHORjkVdm3eF9tL_J5fWEIZ7iQoEZA1nOMt9ouv-eBJLR1bo9e1g0NY9Gf23M7aZrQNq36Ry0bPAK5wRzpMiZk_wyFiITWafCoUNrtmKZvKso8Yx7Bw-XAu47uW8jmMAN7OonbzoTl6gnD6kmVdiVvCtUPbXhM3CVMdL9SgD1tW94y_nfJHRkoOSrrEnvBwewWnyNwasQ_KQy3J8efyCYJlc7D6E0kPqFOYCxyBP7fqvYWoHCBJLntj9r6Smbq85yXLu2yU1L1HNp5An5CHeEurcN1PZ8ue3Cg5ZpaMCMx6pb6C--6w&jsv=sdk_20190107_RC02-production-sdk_20241114_RC00 HTTP/1.1
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
x-afma-drt-cookie: DSID=ACZUy1zwTN84O6zJ6lonl7a-FS1CTlrBElr2Q_aBHCwYD_SlA9NpfUwgQNcxj0ArOoDz4NbGcUfQGn0-VzDHbPVdBVlGvHAPIJ75MLpaCHGbRlgtUx_OBfE
x-afma-drt-v2-cookie: CoIBCnxEU0lEPUFDWlV5MXp3VE44NE82eko2bG9ubDdhLUZTMUNUbHJCRWxyMlFfYUJIQ3dZRF9TbEE5TnBmVXdnUU5jeGowQXJPb0R6NE5iR2NVZlFHbjAtVnpESGJQVmRCVmxHdkhBUElKNzVNTHBhQ0hHYlJsZ3RVeF9PQmZFEAEYAQ==
Host: googleads.g.doubleclick.net

```
Connection: Keep-Alive
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR
IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Afma-Content-Url-Opted-Out: true
X-Afma-Content-Vertical-Opted-Out: true
X-Afma-Analytics-Personalization: true
X-Afma-Use-Https: false
X-Afma-Gws-Query-Id: o1JJZ93cN4aIoPMPjrSJyQI
X-Afma-Mediation: true
Cache-Control: private, no-cache, no-store
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Date: Fri, 29 Nov 2024 05:35:32 GMT
Server: cafe
Content-Length: 153379
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{"ad_type":"","qdata":"x","ad_networks":[{"ad":{"ad_base_url":"https://googleads.g.doubleclick.net","ad_html":"\u003c!DOCTYPE
html\u003e\u003chtml\u003e\u003chead\u003e\u003cmeta charset=\"utf-8\"\u00
...[SNIP]...
```

1.7. https://googleads.g.doubleclick.net/favicon.ico

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/favicon.ico**

Request

```
GET /favicon.ico HTTP/2
Host: googleads.g.doubleclick.net
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like
Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v243799999.231004000.1)
Accept: image/webp,image/apng,image/*,*/*;q=0.8
X-Requested-With: com.datingpro.dolly
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en,en-US;q=0.9
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="static-on-bigtable"
Report-To: {"group":"static-on-bigtable","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/static-on-bigtable"}]}
Content-Length: 1150
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Fri, 22 Nov 2024 20:45:52 GMT
Expires: Sat, 22 Nov 2025 20:45:52 GMT
Cache-Control: public, max-age=31536000
Last-Modified: Thu, 03 Oct 2019 10:15:00 GMT
Content-Type: image/x-icon
Vary: Accept-Encoding
Age: 550151
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

..... .h.......(..... ..... .....|...O...E...M.....lx..4z..?|..@|..
<{..Az....._.....|.....1v..;...?...>}..>z..Cy.....
...[SNIP]...
```

1.8. https://googleads.g.doubleclick.net/getconfig/pubsetting

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/getconfig/pubsetting**

Request

```
GET /getconfig/pubsetting?app_name=com.datingpro.dolly&vnm=102&eid=318502753%2C318515867%2C318516088%2C318516381%2C318516383&js=afma-sdk-a-v243799999.231004000.1&client=ca-app-pub-2489227358200851&admob_appcc=5341356166 HTTP/2
Host: googleads.g.doubleclick.net
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v243799999.231004000.1)
Accept: */*
X-Requested-With: com.datingpro.dolly
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en,en-US;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR
IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
Access-Control-Allow-Origin: https://googleads.g.doubleclick.net
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Date: Fri, 29 Nov 2024 05:35:05 GMT
Server: cafe
Content-Length: 337
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{"status":1,"app_id":"ca-app-pub-2489227358200851~5341356166","auto_collect_location":true,"exp_param":{"loeid":
[44766145]},"publisher_permissions":[{"platform":"ADMOB","eoid_enabled":true,"same_app_k
...[SNIP]...
```

1.9. https://googleads.g.doubleclick.net/mads/gma

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/gma**

Request

```
GET /mads/gma?submodel=sdk_gphone_x86&adid_p=1&format=411x64_as&omid_v=a.1.4.14-
google_20240908&client_purpose_one=false&dv=243799205&ev=22.1.0&hl=en&js=afma-sdk-a-
v243799999.231004000.1&lv=231004600&ms=CpgECoACRfjsdkLkM3pvTf543j95aNwA_FsZktWJnMGbuy4RHmqQHAKu7q9cYr-
84IInXgHEpag1de8BFoOYVUyxEqQIlkDleM0n1pDXK60h0vhh8IcVRnF6MGQ1wtF09YDNnykS3RWAUnPqmFKeofXkIVb4a2Bi
v40YMeMt8YQ27xb7w7gPbXMAFm0DTvv8ricGcZS523bj86jnGvqcsvhoQrlvBOJsq_-kBBbYk102jXcO7Ixc73lyAjUvH-
F8c0CW8UbEXvLBwSyxFwr95CXQcUcxo0XC1eQNai3rf3NUdHKMsHvxKXg2Eh8Ta3nwJokw7Hg-
7OtsxvHwAkMflepJ9CsROgqAAk5IfGAFarilunPo8iLCG2QAP2u-sEEYvIeXVJuaXa-K-
C6UeTdI9A9ayYuhlLzQZzuUO2In6gTOLZmvziPlMRgq0oB_-
IOYlujNGTOCt4q3CKDliUkNzSHoNr28tTumLYUliBGlvBuhYAJb_Vemej53ZSOgKpg-
gmXo2u62iYhSt1ecaTnlCr7iMoMVRQHVNK13ECdk_UnJCwVYAwjXCGiCKfT49mQ6wErmPEirymaB1dAZXUuT7QhXr0CFkYS
CbxN3caZOAcVkSdBRQ2v51qdlZhySY2635ktb3KSBlOPi-
c0b4pwqYGakOy6HBbSDoqAGgfjDZ8OUjg_vJWrawBMSECFDYWgA8SZoY0V5Xjb9G8ASlQIKgAKcbxwiCC3G8WEHWELnGvu-
wPzwmbokMHPjla_aUh5v9akoAtjrmT9Z4NoHHCwhNZT_OX53pOTYKCClLpkAHURYJ71mMUPK7tpQK9vAd_8GK491QeDer
FRk2k6eOPAhmrd6jh7m6QqYGoDNQGjTvqy05atheLzUxQnLEgCYiRW5KjmRjtWmY_hIxK8S-n_sNXC-
BfvJJdLnZf_4GRJ2RXtn7r0xsBL_jRri9dGk7iKhyRxZt-qXqrj2dq5TeeNh-
JIa3BerWTAO50mrmpyKGN10hYAoVXoNtK_jzqoWK3Cu0T9xeNrKU1k0eUrk454mx8HP4PFOa_gy9XAE9wjb0ec9EhA5DX8SsA0J-
NjRzaSUuUmd&mv=84371920.com.android.vending&lft=0&vnm=3.5.7&risd=1&u_sd=2.625&request_id=420502311&rafmt=102&target_api=34&carrier=310260&fbs_aeid=-6234431077831155454&fbs_aiid=e2f6cf45cddfbfd5703631a763303552&seq_num=2&eid=318502753%2C318515867%2C318516088%2C318516381%2C318516383&guci=0.0.0.0.0.0.0.0&adtest=on&sdk_apis=7%2C8&omid_p=Google%2Fafma-sdk-a-
v243799999.231004000.1&u_w=412&u_h=684&msid=com.datingpro.dolly&an=102.android.com.datingpro.dolly&u_audio=4&net=wi&u_so=p&preqs_in_session=1&preqs=1&time_in_session=80&sst=1732858500000&output=html&region=mobile_app&u_tz=-300&client=ca-app-pub-
2489227358200851&slotname=1852091734&gsb=wi&apm_app_id=1%3A20824395699%3Aandroid%3A9d3ef0a0146f0e1a6fc
```

```
5c6&gmp_app_id=1%3A20824395699%3Aandroid%3A9d3ef0a0146f0e1a6fc5c6&apm_app_type=1&lite=0&stbg=1&caps=inlineVideo_interactiveVideo_mraid1_mraid2_mraid3_sdkVideo_exo3_th_autoplay_mediation_scroll_av_transparentBackground_sdkAdmobApiForAds_di_aso_sfv_dinm_dim_nav_navc_dinmo_ipdof_gls_xSeconds&bisch=false&blev=1&canm=false&_mv=84371920.com.android.vending&heap_free=7533165&heap_max=536870912&heap_total=25194957&wv_count=1&rdps=4250&is_lat=false&rdidl=36&idtypel=4&blob=ABPQqLE0W9yupJOE0QEyW0e4sB7CVo-Jp1UgY2fXJXhYRSlsjCgwxXhvUaNh7v2Ed5ktOe5vx3KAhxTgr-acu8TohTYfJ7lEbp-wOZJPQJs00ZinyvDgwZXuhoS9afd8K8GW8cUULPGV-60xmRz0lIeRDyFl8epkW7djgMcJll1xh5XRggCO_M0sfFpUajnDH_DFBwElL9pjNKgKAk-Dwv6rC6PQQBv2iqasOj2iQ76XUpyg_sX5Ycs1ixHi39pEqALLE5Wa2W42LcoIYIzRuavAFxVjQeNhQANXbjgiGg5c64rXartnU3o0FNUTwQ&adk=2603848924&jsv=sdk_20190107_RC02-production-sdk_20241114_RC00 HTTP/1.1
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
x-afma-drt-cookie: DSID=ACZUy1zwTN84O6zJ6lonl7a-FS1CTlrBElr2Q_aBHCwYD_SlA9NpfUwgQNcxj0ArOoDz4NbGcUfQGn0-VzDHbPVdBVlGvHAPIJ75MLpaCHGbRlgtUx_OBfE
x-afma-drt-v2-cookie: CoIBCnxEU0lEPUFDWlV5MXp3VE44NE82eko2bG9ubDdhLUZTMUNUbHJCRWxyMlFfYUJIQ3dZRF9TbEE5TnBmVXdnUU5jeGowQXJPb0R6NE5iR2NVZlFHbjAtVnpESGJQVmRCVmxHdkhBUElKNzVNTHBhQ0hHYlJsZ3RVeF9PQmZFEAEYAQ==
Host: googleads.g.doubleclick.net
Connection: Keep-Alive
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Afma-Analytics-Personalization: true
X-Afma-Content-Vertical-Opted-Out: true
X-Afma-Content-Url-Opted-Out: true
X-Afma-Use-Https: false
X-Afma-Gws-Query-Id: o1JJZ67mN9-zoPMP-8DW6Q4
X-Afma-Mediation: true
Cache-Control: private, no-cache, no-store
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Date: Fri, 29 Nov 2024 05:35:32 GMT
Server: cafe
Content-Length: 131799
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{"ad_type":"banner","qdata":"x","ad_networks":[{"ad":{"ad_base_url":"https://googleads.g.doubleclick.net","ad_html":"\u003c!DOCTYPE html\u003e\u003chtml lang=en\u003e\u003chead\u003e\u003cmeta charset
...[SNIP]...
```

1.10. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://googleads.g.doubleclick.net**

Path: **/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html**

Request

```
GET /mads/static/mad/sdk/native/production/sdk-core-v40-impl.html HTTP/2
Host: googleads.g.doubleclick.net
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v243799999.231004000.1)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
X-Requested-With: com.datingpro.dolly
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en,en-US;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Content-Type-Options: nosniff
Server: cafe
Content-Length: 387132
X-Xss-Protection: 0
Date: Fri, 29 Nov 2024 05:23:43 GMT
Expires: Sat, 30 Nov 2024 05:23:43 GMT
Cache-Control: public, max-age=86400
Age: 679
Etag: 4395789294679574262
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

<!DOCTYPE html>
<html>
<head>
<script>
(function (){ /*

Copyright The Closure Library Authors.
SPDX-License-Identifier: Apache-2.0
*/
/*

Copyright 2011 Google Inc. All rights reserved.
Lic
...[SNIP]...
```

1.11. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js**

Request

```
GET /mads/static/mad/sdk/native/production/sdk-core-v40-impl.js?n=true&lv=sdk_20190107_RC02 HTTP/2
Host: googleads.g.doubleclick.net
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
Accept: */*
X-Requested-With: com.google.android.gms
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Server: cafe
Content-Length: 537947
X-Xss-Protection: 0
Date: Fri, 29 Nov 2024 02:02:38 GMT
Expires: Fri, 29 Nov 2024 06:02:38 GMT
Cache-Control: public, max-age=14400
Age: 12747
Etag: 9673142243471861567
Content-Type: text/javascript; charset=UTF-8
Vary: Accept-Encoding
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

(function (){ /*

Copyright The Closure Library Authors.
SPDX-License-Identifier: Apache-2.0
*/
/*

Copyright 2011 Google Inc. All rights reserved.
```

Licensed under the Apache License, Versi
...[SNIP]...

1.12. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.appcache

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/static/mad/sdk/native/sdk-core-v40-loader.appcache**

Request

```
GET /mads/static/mad/sdk/native/sdk-core-v40-loader.appcache HTTP/2
Host: googleads.g.doubleclick.net
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
Accept: */*
X-Requested-With: com.google.android.gms
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Content-Type-Options: nosniff
Server: cafe
Content-Length: 192
X-Xss-Protection: 0
Date: Fri, 29 Nov 2024 05:25:49 GMT
Expires: Fri, 29 Nov 2024 07:25:49 GMT
Cache-Control: public, max-age=7200
Age: 582
Etag: 16027413122022871166
Content-Type: text/cache-manifest; charset=UTF-8
Vary: Accept-Encoding
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

CACHE MANIFEST
/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js

NETWORK:
*
```

```
# AppCache versioning info below:
# pid = 0e1c42b3-e0ba-4b09-b3b8-99192dc8b2ad
# cn = sdk_20241120_RC00
```

1.13. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/static/mad/sdk/native/sdk-core-v40-loader.html**

Request

```
GET /mads/static/mad/sdk/native/sdk-core-v40-loader.html HTTP/2
Host: googleads.g.doubleclick.net
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
X-Requested-With: com.google.android.gms
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
Vary: Accept-Encoding
Date: Fri, 29 Nov 2024 05:35:05 GMT
Expires: Fri, 29 Nov 2024 05:35:05 GMT
Cache-Control: private, max-age=86400
Content-Type: text/html; charset=UTF-8
Etag: 16295587571342835724
X-Content-Type-Options: nosniff
Server: cafe
Content-Length: 196
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000


<!DOCTYPE html>
<html>
<head>
```

```
<script>
var efs = false;
</script>
<script src="/mads/static/mad/sdk/native/sdk-core-v40-loader.js"></script>
</head>
<body></body>
</html>
```

1.14. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.js

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/static/mad/sdk/native/sdk-core-v40-loader.js**

Request

```
GET /mads/static/mad/sdk/native/sdk-core-v40-loader.js HTTP/2
Host: googleads.g.doubleclick.net
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
Accept: */*
X-Requested-With: com.google.android.gms
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Server: cafe
Content-Length: 47613
X-Xss-Protection: 0
Date: Fri, 29 Nov 2024 04:47:09 GMT
Expires: Fri, 29 Nov 2024 08:47:09 GMT
Cache-Control: public, max-age=14400
Age: 2876
Etag: 11080626372616993405
Content-Type: text/javascript; charset=UTF-8
Vary: Accept-Encoding
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

```
// Copyright 2013 Google Inc. All Rights Reserved.
(function(){var aa="DOMContentLoaded",ba="Storage mechanism: Invalid value was encountered",ca="Storage: Invalid value was encountered",da="canary-ex
...[SNIP]...
```

1.15. https://tnzslk-launches.appsflyersdk.com/api/v6.12/androidevent

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://tnzslk-launches.appsflyersdk.com**
Path:	**/api/v6.12/androidevent**

Issue detail

This issue was found in multiple locations under the reported path.

Request

```
POST /api/v6.12/androidevent?app_id=com.datingpro.dolly&buildnumber=6.12.1 HTTP/1.1
Content-Type: application/octet-stream
Content-Length: 1912
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; sdk_gphone_x86 Build/RSR1.201013.001)
Host: tnzslk-launches.appsflyersdk.com
Connection: Keep-Alive
Accept-Encoding: gzip, deflate, br

....AE-I..{Kh.\......0.w.X?....!..#@........SIZ.`M.8...W...Jd5u.3~...A..[..S.F.I.R...j.[.5iK.....#VyBO..&...)...W...g&........1...j|M....V.sa.I
   ..6...&..b..S+X=..
!....Q>vg..u...F..M......aN..r.._|..
...[SNIP]...
```

Response

```
HTTP/2 403 Forbidden
Content-Length: 9
Date: Fri, 29 Nov 2024 05:34:54 GMT
X-Cache: Error from cloudfront
Via: 1.1 5f928efc6cc9f0bbea9fe5327d80c446.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C1
X-Amz-Cf-Id: lTyFRclDh21wECDORrBiYR1UZmPDtrX2nXVBS2H15WtiZUGp2BaxLw==

forbidden
```

1.16. https://www.deliverizate.es/

Summary

Severity:	**Low**

Confidence: **Certain**

Host: **https://www.deliverizate.es**

Path: **/**

Issue detail

This issue was found in multiple locations under the reported path.

Request

```
GET /storage/thumbnails/1715041657IMG_20240403_183337.jpg HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; sdk_gphone_x86 Build/RSR1.201013.001)
Host: www.deliverizate.es
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 29 Nov 2024 05:35:03 GMT
Server: Apache/2.4.52 (Ubuntu)
Last-Modified: Tue, 07 May 2024 00:27:38 GMT
ETag: "4871-617d240d5b7cf"
Accept-Ranges: bytes
Content-Length: 18545
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: image/jpeg

......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 50
...C......
........(.....1#%.(:3=<9387@H\N@DWE78PmQW_bghg>Mqypdx\egc...C......./../cB8Bccccccccccccccccccccccccccccccc
...[SNIP]...
```

1.17. https://www.deliverizate.es/api/getUserInfo

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://www.deliverizate.es**

Path: **/api/getUserInfo**

Request

```
POST /api/getUserInfo HTTP/1.1
Host: www.deliverizate.es
Content-Type: application/json;
Content-Length: 33
Accept-Encoding: gzip, deflate, br
User-Agent: okhttp/5.0.0-alpha.2
```

```
Connection: keep-alive

{"fb_id":"101754338164003873967"}
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 29 Nov 2024 05:35:02 GMT
Server: Apache/2.4.52 (Ubuntu)
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 56
Access-Control-Allow-Origin: *
Content-Length: 880
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json

{"code":"200","msg":
[{"fb_id":"101754338164003873967","about_me":"","audio":"","audio_prompt":"","gender":"0","birthday":"11\/29\/1995","age":29,"
first_name":"SOEN321","last_name":"","living":0,"child
...[SNIP]...
```

1.18. https://www.deliverizate.es/api/saveImageF

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://www.deliverizate.es**
Path:	**/api/saveImageF**

Request

```
POST /api/saveImageF HTTP/1.1
Host: www.deliverizate.es
Content-Type: multipart/form-data; boundary=fa92612c-ddc2-4ff2-9749-129e341db840
Content-Length: 1200000
Accept-Encoding: gzip, deflate, br
User-Agent: okhttp/5.0.0-alpha.2
Connection: keep-alive

--fa92612c-ddc2-4ff2-9749-129e341db840
Content-Disposition: form-data; name="image"; filename="premium_photo-1671656349322-41de944d259b.jpeg"
Content-Type: multipart/form-data
Content-Length: 11997
...[SNIP]...
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 29 Nov 2024 05:34:44 GMT
Server: Apache/2.4.52 (Ubuntu)
Cache-Control: no-cache, private
```

```
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
Access-Control-Allow-Origin: *
Content-Length: 155
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json

{"code":"200","msg":[{"success":true,"file":"https:\/\/www.deliverizate.es\/storage\/mainimage\/1732858484premium_photo-1671656349322-41de944d259b.jpeg"}]}
```

1.19. https://www.deliverizate.es/api/signup

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://www.deliverizate.es**
Path:	**/api/signup**

Request

```
POST /api/signup HTTP/1.1
Host: www.deliverizate.es
Content-Type: application/json;
Content-Length: 312
Accept-Encoding: gzip, deflate, br
User-Agent: okhttp/5.0.0-alpha.2
Connection: keep-alive

{"fb_id":"10175433816400387396 7","first_name":"SOEN321","birthday":"11\/29\/1995","gender":"0","minage":"19","maxage":"39","genderfind":"1","lookfor":"78","disability":"3","signupfrom":"google","image
...[SNIP]...
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 29 Nov 2024 05:34:46 GMT
Server: Apache/2.4.52 (Ubuntu)
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 58
Access-Control-Allow-Origin: *
Content-Length: 417
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: application/json

{"code":"200","msg":
[{"fb_id":"10175433816400387396 7","first_name":"SOEN321","last_name":"","disability":"3","birthday":"11\/29\/1995","age":29,"image1":"https:\/\/www.deliverizate.es\/storage\/mainim
...[SNIP]...
```

1.20. https://www.deliverizate.es/api/userNearByMePageFilters

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://www.deliverizate.es**

Path: **/api/userNearByMePageFilters**

Request

```
POST /api/userNearByMePageFilters HTTP/1.1
Host: www.deliverizate.es
Content-Type: application/json;
Content-Length: 686
Accept-Encoding: gzip, deflate, br
User-Agent: okhttp/5.0.0-alpha.2
Connection: keep-alive

{"fb_id":"10175433816400387 3967","lat_long":"37.4219983,
-122.084","gender":"1","relationship":"","distance":"10000","device_token":"fcklSmKVSiiHSvndvXr01v:APA91bHiiA44QHJmtuSR
DrwRWqvhQs-QfJiytLnU56O4
...[SNIP]...
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 29 Nov 2024 05:35:02 GMT
Server: Apache/2.4.52 (Ubuntu)
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 55
Access-Control-Allow-Origin: *
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json
Content-Length: 31098

{"code":"200","page":1,"page_limit":9,"msg":
[{"fb_id":"12533396944","first_name":"Cass","last_name":"","birthday":"20","about_me":"","audio":"","audio_prompt":"","distance"
:"676 miles away","km":676,"
...[SNIP]...
```

1.21. https://www.deliverizate.es/storage/mainimage/1731198209IMG_20241109_162327800.jpg

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://www.deliverizate.es**

Path: **/storage/mainimage/1731198209IMG_20241109_162327800.jpg**

Request

```
GET /storage/mainimage/1731198209IMG_20241109_162327800.jpg HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; sdk_gphone_x86 Build/RSR1.201013.001)
Host: www.deliverizate.es
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 29 Nov 2024 05:35:03 GMT
Server: Apache/2.4.52 (Ubuntu)
Last-Modified: Sun, 10 Nov 2024 00:23:29 GMT
ETag: "aea9-62683fe4eb3c1"
Accept-Ranges: bytes
Content-Length: 44713
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: image/jpeg

......JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 60
...C.
.
..
..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.......&..&O5-
5OOOOOOOOOOOOOOOOOOOOOOOOOOOOO
...[SNIP]...
```

1.22. https://www.deliverizate.es/storage/mainimage/1732858484premium_photo-1671656349322-41de944d259b.jpeg

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://www.deliverizate.es**

Path: **/storage/mainimage/1732858484premium_photo-1671656349322-41de944d259b.jpeg**

Request

```
GET /storage/mainimage/1732858484premium_photo-1671656349322-41de944d259b.jpeg HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; sdk_gphone_x86 Build/RSR1.201013.001)
Host: www.deliverizate.es
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 29 Nov 2024 05:35:02 GMT
Server: Apache/2.4.52 (Ubuntu)
Last-Modified: Fri, 29 Nov 2024 05:34:45 GMT
ETag: "5da8-628068e77d06a"
Accept-Ranges: bytes
Content-Length: 23976
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/jpeg

.....JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 60
...C.
.
..
..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.......&..&O5-
5OOOOOOOOOOOOOOOOOOOOOOOOOOOOO
...[SNIP]...
```

1.23. https://www.deliverizate.es/storage/thumbnails/1731198209IMG_20241109_162327800.jpg

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://www.deliverizate.es**
Path:	**/storage/thumbnails/1731198209IMG_20241109_162327800.jpg**

Request

```
GET /storage/thumbnails/1731198209IMG_20241109_162327800.jpg HTTP/1.1
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; sdk_gphone_x86 Build/RSR1.201013.001)
Host: www.deliverizate.es
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 29 Nov 2024 05:35:03 GMT
Server: Apache/2.4.52 (Ubuntu)
Last-Modified: Sun, 10 Nov 2024 00:23:30 GMT
ETag: "6b44-62683fe5a0e01"
Accept-Ranges: bytes
Content-Length: 27460
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: image/jpeg

.....JFIF.....`.`.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 50
```

...C.....
.....(.....1#%.(:3=<9387@H\N@DWE78PmQW_bghg>Mqypdx\egc...C...../../cB8Bccccccccccccccccccccccccccccc
...[SNIP]...

---

2. Cookie scoped to parent domain

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://img.onesignal.com**
Path:	**/i/b9accb0d-d46d-4743-88fb-12fe15de37e9/KDM4VvFTXuZ6EcH5id4O_clasificacion.gif**

Issue detail

The following cookie was issued by the application and is scoped to a parent of the issuing domain:

- __cf_bm

The cookie does not appear to contain a session token, which may reduce the risk associated with this issue. You should review the contents of the cookie to determine its function.

Issue background

A cookie's domain attribute determines which domains can access the cookie. Browsers will automatically submit the cookie in requests to in-scope domains, and those domains will also be able to access the cookie via JavaScript. If a cookie is scoped to a parent domain, then that cookie will be accessible by the parent domain and also by any other subdomains of the parent domain. If the cookie contains sensitive data (such as a session token) then this data may be accessible by less trusted or less secure applications residing at those domains, leading to a security compromise.

Issue remediation

By default, cookies are scoped to the issuing domain, and on IE/Edge to subdomains. If you remove the explicit domain attribute from your Set-cookie directive, then the cookie will have this default scope, which is safe and appropriate in most situations. If you particularly need a cookie to be accessible by a parent domain, then you should thoroughly review the security of the applications residing on that domain and its subdomains, and confirm that you are willing to trust the people and systems that support those applications.

Vulnerability classifications

- CWE-16: Configuration

Request

```
GET /i/b9accb0d-d46d-4743-88fb-12fe15de37e9/KDM4VvFTXuZ6EcH5id4O_clasificacion.gif HTTP/1.1
Host: img.onesignal.com
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
X-Requested-With: com.datingpro.dolly
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Accept-Encoding: gzip, deflate, br
Accept-Language: en,en-US;q=0.9
```

```
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 05:33:35 GMT
Content-Type: image/gif
Content-Length: 2194244
Cache-Control: public, max-age=2678400
Cf-Bgj: imgq:85,h2pri
Cf-Polished: origSize=2315699, status=vary_header_present
Alt-Svc: h3=":443"; ma=86400
Etag: "-CNWJ+Znj44gDEAE="
Expires: Mon, 30 Dec 2024 05:33:35 GMT
Last-Modified: Fri, 27 Sep 2024 18:41:15 GMT
Pragma: no-cache
Vary: Origin, Accept-Encoding
X-Goog-Encryption-Kms-Key-Name: projects/core-infra-onesignal/locations/europe-west4/keyRings/keyring-kms-onesignal/cryptoKeys/img-persistence-bucket-onesignal/cryptoKeyVersions/1
X-Goog-Generation: 1727462475973845
X-Goog-Hash: crc32c=DsFWDA==
X-Goog-Hash: md5=c3nk4+9vvJP2mt3WnoLH4w==
X-Goog-Metageneration: 1
X-Goog-Storage-Class: STANDARD
X-Goog-Stored-Content-Encoding: identity
X-Goog-Stored-Content-Length: 2315699
X-Guploader-Uploadid: AFiumC5efnbmu2g-UnNs3BtImSqmYwlIOQCSObkNeIWHsToFVWc5LBNncyqZbszYYggXshMleYqdx5_vdA
Cf-Cache-Status: HIT
Accept-Ranges: bytes
Set-Cookie: __cf_bm=l.AExG_QmfdhjzkTJbXzL7SiDy2d8Y8lszvvqZZPY8s-1732858415-1.0.1.1-iBZ17iBV.q9FtvkprVb7pPPT4XkSTNXyM2quOQpt6IMek.dFIHEPSlXMGxBN2rnpu4z4uBbk8x49tXK2Tm9hKQ; path=/; expires=Fri, 29-Nov-24 06:03:35 GMT; domain=.onesignal.com; HttpOnly; Secure; SameSite=None
Strict-Transport-Security: max-age=15552000; includeSubDomains
Server: cloudflare
Cf-Ray: 8ea03947db27a2ce-YUL

GIF89a.....3.....  .....@@@b..7.....?.....+++Y.....pppBBB.....###;;;.....VVV...XXX...V.....
.....<<<...}..fff.....777===.....L
...[SNIP]...
```

---

3. Cross-domain Referer leakage

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://fonts.googleapis.com**
Path:	**/css**

Issue detail

The page was loaded from a URL containing a query string:

- https://fonts.googleapis.com/css

The response contains the following links to other domains:

- https://developers.google.com/fonts/docs/getting_started
- https://www.google.com/fonts
- https://www.google.com/images/logos/google_logo_41.png

Issue background

When a web browser makes a request for a resource, it typically adds an HTTP header, called the "Referer" header, indicating the URL of the resource from which the request originated. This occurs in numerous situations, for example when a web page loads an image or script, or when a user clicks on a link or submits a form.

If the resource being requested resides on a different domain, then the Referer header is still generally included in the cross-domain request. If the originating URL contains any sensitive information within its query string, such as a session token, then this information will be transmitted to the other domain. If the other domain is not fully trusted by the application, then this may lead to a security compromise.

You should review the contents of the information being transmitted to other domains, and also determine whether those domains are fully trusted by the originating application.

Today's browsers may withhold the Referer header in some situations (for example, when loading a non-HTTPS resource from a page that was loaded over HTTPS, or when a Refresh directive is issued), but this behavior should not be relied upon to protect the originating URL from disclosure.

Note also that if users can author content within the application then an attacker may be able to inject links referring to a domain they control in order to capture data from URLs used within the application.

Issue remediation

Applications should never transmit any sensitive information within the URL query string. In addition to being leaked in the Referer header, such information may be logged in various locations and may be visible on-screen to untrusted parties. If placing sensitive information in the URL is unavoidable, consider using the Referer-Policy HTTP header to reduce the chance of it being disclosed to third parties.

References

- Referer Policy
- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-200: Information Exposure

Request

```
GET /css?family=System%20Font%20(Default)|System%20Font%20(Default)|System%20Font%20(Default) HTTP/2
Host: fonts.googleapis.com
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36
Accept: text/css,*/*;q=0.1
X-Requested-With: com.datingpro.dolly
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: style
Accept-Encoding: gzip, deflate, br
Accept-Language: en,en-US;q=0.9
```

Response

```
HTTP/2 400 Bad Request
Content-Type: text/html; charset=utf-8
```

```
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Mon, 01 Jan 1990 00:00:00 GMT
Date: Fri, 29 Nov 2024 05:33:35 GMT
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy: same-origin-allow-popups
Server: ESF
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

<!DOCTYPE html><html lang=en><head><meta charset=utf-8><title>400: Font family not found</title><link
href="//fonts.googleapis.com/css?family=Open+Sans:300,400" rel="stylesheet" type="text/css"/><styl
...[SNIP]...
<ins>For reference, see the <a href="https://developers.google.com/fonts/docs/getting_started">Google Fonts API
documentation</a>
...[SNIP]...
```

---

4. Frameable response (potential Clickjacking)

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/static/mad/sdk/native/sdk-core-v40-loader.html**

Issue description

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.

You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.

Issue remediation

To effectively prevent framing attacks, the application should return a response header with the name **X-Frame-Options** and the value **DENY** to prevent framing altogether, or the value **SAMEORIGIN** to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.

References

- Web Security Academy: Clickjacking
- X-Frame-Options

Vulnerability classifications

- CWE-693: Protection Mechanism Failure
- CWE-1021: Improper Restriction of Rendered UI Layers or Frames
- CAPEC-103: Clickjacking

Request

```
GET /mads/static/mad/sdk/native/sdk-core-v40-loader.html HTTP/2
Host: googleads.g.doubleclick.net
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
X-Requested-With: com.google.android.gms
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
Vary: Accept-Encoding
Date: Fri, 29 Nov 2024 05:35:05 GMT
Expires: Fri, 29 Nov 2024 05:35:05 GMT
Cache-Control: private, max-age=86400
Content-Type: text/html; charset=UTF-8
Etag: 16295587571342835724
X-Content-Type-Options: nosniff
Server: cafe
Content-Length: 196
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000


<!DOCTYPE html>
<html>
<head>
<script>
var efs = false;
</script>
<script src="/mads/static/mad/sdk/native/sdk-core-v40-loader.js"></script>
</head>
<body></body>
</html>
```

---

5. Browser cross-site scripting filter disabled

There are 12 instances of this issue:

- https://dl.google.com/vision/1/creditcard/gocr_credit_card_ocr_v0.zip
- https://fonts.googleapis.com/css
- https://fundingchoicesmessages.google.com/a/consent
- https://googleads.g.doubleclick.net/
- https://googleads.g.doubleclick.net/favicon.ico
- https://googleads.g.doubleclick.net/getconfig/pubsetting
- https://googleads.g.doubleclick.net/mads/gma
- https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html
- https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js
- https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.appcache
- https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html
- https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.js

Issue description

Some browsers, including Internet Explorer, contain built-in filters designed to protect against cross-site scripting (XSS) attacks. Applications can instruct browsers to disable this filter by setting the following response header:

X-XSS-Protection: 0

This behavior does not in itself constitute a vulnerability; in some cases XSS filters may themselves be leveraged to perform attacks against application users. However, in typical situations XSS filters do provide basic protection for application users against some XSS vulnerabilities in applications. The presence of this header should be reviewed to establish whether it affects the application's security posture.

Issue remediation

Review whether the application needs to disable XSS filters. In most cases you can gain the protection provided by XSS filters without the associated risks by using the following response header:

X-XSS-Protection: 1; mode=block

When this header is set, browsers that detect an XSS attack will simply render a blank page instead of attempting to sanitize the injected script. This behavior is considerably less likely to introduce new security issues.

References

- Web Security Academy: Cross-site scripting
- Controlling the XSS Filter

Vulnerability classifications

- CWE-16: Configuration
- CAPEC-63: Cross-Site Scripting (XSS)

5.1. https://dl.google.com/vision/1/creditcard/gocr_credit_card_ocr_v0.zip

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://dl.google.com**

Path: **/vision/1/creditcard/gocr_credit_card_ocr_v0.zip**

Request

```
GET /vision/1/creditcard/gocr_credit_card_ocr_v0.zip HTTP/2
Host: dl.google.com
User-Agent: com.google.android.gms/244534025 (Linux; U; Android 11; en_US; sdk_gphone_x86; Build/RSR1.201013.001; Cronet/132.0.6779.0)
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Disposition: attachment
Content-Security-Policy: default-src 'none'
Server: downloads
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 0
Date: Fri, 29 Nov 2024 05:35:31 GMT
Cache-Control: public,max-age=86400
Last-Modified: Fri, 21 Oct 2022 23:56:48 GMT
Etag: "fd7fee"
Content-Type: application/zip
Content-Length: 696543
Age: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

PK.....!()(x.....credit_card_ocr_engine.binarypb.T]k.A.e..uj?..b..].-E..M.m@..m.4M.)(.....]..Yfg.....D.....?A_|.._..n..h>...
{..s.=w.....].[...I...|A.^    8.....9/b..I.H..+;.....&-.f.!
...[SNIP]...
```

5.2. https://fonts.googleapis.com/css

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://fonts.googleapis.com**

Path: **/css**

Request

```
GET /css?family=System%20Font%20(Default)|System%20Font%20(Default)|System%20Font%20(Default) HTTP/2
Host: fonts.googleapis.com
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36
Accept: text/css,*/*;q=0.1
X-Requested-With: com.datingpro.dolly
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
```

```
Sec-Fetch-Dest: style
Accept-Encoding: gzip, deflate, br
Accept-Language: en,en-US;q=0.9
```

Response

```
HTTP/2 400 Bad Request
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Mon, 01 Jan 1990 00:00:00 GMT
Date: Fri, 29 Nov 2024 05:33:35 GMT
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy: same-origin-allow-popups
Server: ESF
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

<!DOCTYPE html><html lang=en><head><meta charset=utf-8><title>400: Font family not found</title><link
href="//fonts.googleapis.com/css?family=Open+Sans:300,400" rel="stylesheet" type="text/css"/><styl
...[SNIP]...
```

5.3. https://fundingchoicesmessages.google.com/a/consent

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://fundingchoicesmessages.google.com**
Path:	**/a/consent**

Request

```
POST /a/consent HTTP/1.1
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like
Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36
Content-Type: application/json
Host: fundingchoicesmessages.google.com
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
Content-Length: 448

{"admob_app_id":"ca-app-pub-2489227358200851~5341356166","is_lat":false,"adid":"f20fbe71-dba0-4c12-8b2e-
6cbbc3d4cdfe","device_info":{"os_type":"ANDROID","model":"sdk_gphone_x86","android_api_level":30
...[SNIP]...
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
X-Content-Type-Options: nosniff
```

Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Mon, 01 Jan 1990 00:00:00 GMT
Date: Fri, 29 Nov 2024 05:35:02 GMT
Content-Disposition: attachment; filename="json.txt"; filename*=UTF-8''json.txt
Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/ContributorServingAppSwitchboardHttp/cspreport
Content-Security-Policy: script-src 'report-sample' 'nonce-v2wT9LASY56K_F2eueDIZg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/ContributorServingAppSwitchboardHttp/cspreport;worker-src 'self'
Content-Security-Policy: script-src 'unsafe-inline' 'unsafe-eval' blob: data: 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.googletagmanager.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/ContributorServingAppSwitchboardHttp/cspreport/allowlist
Accept-Ch: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-WoW64, Sec-CH-UA-Form-Factors, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version
Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-wow64=*, ch-ua-form-factors=*, ch-ua-platform=*, ch-ua-platform-version=*
Cross-Origin-Opener-Policy: same-origin
Reporting-Endpoints: default="/_/ContributorServingAppSwitchboardHttp/web-reports?context=eJzjStDikmLw1pBikPj6kkkDiJ3SZ7AGAXHrzXOsU4E46d951iIgNlS4xOoIwkWXWD2BWLXnEqspEN9fd4n1ORDPOH-ZdQEQF0IcYW0CYoavV1g5gFiIh6Nt6dJdbAI3bi18zaikkZRfGJ-cn1dSlJlUWpJflJacllqcWlSWWhRvZGBkYmhoaKlnYBhfYAAA4Gs9jw"
Server: ESF
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

)]}'
{
"consent_signal": "CONSENT_SIGNAL_NOT_REQUIRED",
"consent_form_base_url": "about:blank/",
"request_info_keys": ["IABTCF_TCString", "IABTCF_AddtlConsent", "IABTCF_idfaFlowControl", "IDFA_f
...[SNIP]...

5.4. https://googleads.g.doubleclick.net/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/**

Issue detail

This issue was found in multiple locations under the reported path.

Request

GET /mads/gma?submodel=sdk_gphone_x86&adid_p=1&format=interstitial_mb&omid_v=a.1.4.14-google_20240908&client_purpose_one=false&dv=243799205&ev=22.1.0&hl=en&js=afma-sdk-a-v243799999.231004000.1&lv=231004600&ms=CpgECoACRfDsdkLgM3pvTf543jF5aNwK_FsZltWJnMebuy4VHmqQHgKu7q1cYr-w4lInWAHEpaY1de8DFoOYV0yxEqoIlkDpeM0n0pDXK6sh0vhr8IcVQnF6MG41wtF09YDNkSkS3ReAUnPsmFKeo_XkIVL4a2Bqv40YOeMt8YA27xb9w7gPb3MAFmMDTvv8ricGdZS5237j86jtGvqcuPhoQr1vBOJkq_-kABbYk1c2jXcO7Ixc5XlyAjcvH-Fwc0CW8UbEXvLBwSy_Fwr94iXQcUsxo0XI1eQNYC3rf3tUdHKAsHvxK3g2EhMTa3n8Jokw4Hg-7OtsxvH4AkMfkepJ9CEROgqAAouyqEZjTD1U-KRw7Vfq9kRX0yMhCulSOshe3oLgMwyi74fI_uXlaxM5DQnYPH20Lc3xG2stEpXxp4hdsJrrbD9m7Z0xnLWLwE8vsb6NMWS2Y3Uu6bh3I5AePj5DM4-snFuhzxzgG6MikOzCps7pjTswaIhn63xperuTq63DGn4JQc3z4iFLqJ-Gc77p1p-

```
w5fG39Bq5J1W9854FVR2Vp35QX4RZiLtpPIRO7G5QJTosP8FxFXPLwmGxWsFQHZ6TJng1uBmloLBiS-
Gudm35WXfIOEFdj2q7G4FUeliqo0KynpLhq06HKYi5l3x4lWiWkZbWOyM2tPMLF_pOaRg7ZIQSEKI6D4fWKdQYbWUbG47ZKv
4SlQIKgALwk4mbIQMYmOi1dxKEEjD9DBRpD9oyAu_oCkcknszXA-
BeM1lXHawwLMtZ_90ltPfv6k81kaY78Nlo6oqglnBWDdSwDw0qA5lvhjvcHeoHOuKAS8JIVwfrs1e3OZQaaDc6ULU43qybe7AAA
j0zBtG91pFH1sqlq-
bjMLg0jKnHLYimrnwXBKKZUtKQI80qZNobipC4OKjFSkidzn_zufLiMIgJ9KOYxkBKcTZH9x7LE5am6oozeHiYntSmt345ajwa-
8wF3K0VkVin7-_v31mF5ZDL5PEFH-18PZZElsBOlbiqFP7F1IbdDhCTpI9PlJKVH2pB5TTeyTQdDe7zKUyOEhA5DX8SsA0J-
NjRzaSUuUmd&mv=84371920.com.android.vending&lft=0&vnm=3.5.7&risd=1&u_sd=2.625&request_id=202454318&target_ap
i=34&carrier=310260&fbs_aeid=-6234431077831155455&fbs_aiid=e2f6cf45cddfbfd5703631a763303552&seq_num=1&eid=31
8502753%2C318515867%2C318516088%2C318516381%2C318516383&guci=0.0.0.0.0.0.0.0&adtest=on&sdk_apis=7%2C8&
omid_p=Google%2Fafma-sdk-a-
v243799999.231004000.1&u_w=412&u_h=684&msid=com.datingpro.dolly&an=102.android.com.datingpro.dolly&u_audio=4&n
et=wi&u_so=p&preqs_in_session=0&preqs=0&time_in_session=0&sst=1732858500000&output=html&region=mobile_app&u_t
z=-300&client=ca-app-pub-
2489227358200851&slotname=2809117006&gsb=wi&apm_app_id=1%3A20824395699%3Aandroid%3A9d3ef0a0146f0e1a6fc
5c6&gmp_app_id=1%3A20824395699%3Aandroid%3A9d3ef0a0146f0e1a6fc5c6&apm_app_type=1&lite=0&num_ads=1&vpt=8
&vfmt=18&vst=0&sdkv=o.243799999.231004000.1&sdmax=0&dmax=1&sdki=3c4d&stbg=1&caps=inlineVideo_interactiveVideo
_mraid1_mraid2_mraid3_sdkVideo_exo3_th_autoplay_mediation_scroll_av_transparentBackground_sdkAdmobApiForAds_di_
aso_sfv_dinm_dim_nav_navc_dinmo_ipdof_gls_xSeconds&bisch=false&blev=1&canm=false&_mv=84371920.com.android.ven
ding&heap_free=8095765&heap_max=536870912&heap_total=25194957&wv_count=1&rdps=4250&is_lat=false&rdidl=36&idty
pel=4&blob=ABPQqLGGVg2RHORjkVdm3eF9tL_J5fWEIZ7iQoEZA1nOMt9ouv-
eBJLR1bo9e1g0NY9Gf23M7aZrQNq36Ry0bPAK5wRzpMiZk_wyFiITWafCoUNrtmKZvKso8Yx7Bw-
XAu47uW8jmMAN7OonbzoTl6gnD6kmVdiVvCtUPbXhM3CVMdL9SgD1tW94y_nfJHRkoOSrrEnvBwewWnyNwasQ_KQy3J8efy
CYJlc7D6E0kPqFOYCxyBP7fqvYWoHCBJLntj9r6Smbq85yXLu2yU1L1HNp5An5CHeEurcN1PZ8ue3Cg5ZpaMCMx6pb6C-
-6w&jsv=sdk_20190107_RC02-production-sdk_20241114_RC00 HTTP/1.1
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like
Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
x-afma-drt-cookie: DSID=ACZUy1zwTN84O6zJ6lonI7a-
FS1CTlrBElr2Q_aBHCwYD_SlA9NpfUwgQNcxj0ArOoDz4NbGcUfQGn0-VzDHbPVdBVlGvHAPlJ75MLpaCHGbRlgtUx_OBfE
x-afma-drt-v2-cookie:
CoIBCnxEU0lEPUFDWlV5MXp3VE44NE82eko2bG9ubDdhLUZTMUNUbHJCRWxyMlFfYUJIQ3dZRF9TbEE5TnBmVXdnUU5j
eGowQXJPb0R6NE5iR2NVZlFHbjAtVnpESGJQVmRCVmxHdkhBUElKNzVNTHBhQ0hHYlJsZ3RVeF9PQmZFEAEYAQ==
Host: googleads.g.doubleclick.net
Connection: Keep-Alive
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR
IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Afma-Content-Url-Opted-Out: true
X-Afma-Content-Vertical-Opted-Out: true
X-Afma-Analytics-Personalization: true
X-Afma-Use-Https: false
X-Afma-Gws-Query-Id: o1JJZ93cN4aIoPMPjrSJyQI
X-Afma-Mediation: true
Cache-Control: private, no-cache, no-store
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Date: Fri, 29 Nov 2024 05:35:32 GMT
Server: cafe
Content-Length: 153379
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{"ad_type":"","qdata":"x","ad_networks":[{"ad":{"ad_base_url":"https://googleads.g.doubleclick.net","ad_html":"\u003c!DOCTYPE
html\u003e\u003chtml\u003e\u003chead\u003e\u003cmeta charset=\"utf-8\"\u00
...[SNIP]...
```

5.5. https://googleads.g.doubleclick.net/favicon.ico

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/favicon.ico**

Request

```
GET /favicon.ico HTTP/2
Host: googleads.g.doubleclick.net
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v243799999.231004000.1)
Accept: image/webp,image/apng,image/*,*/*;q=0.8
X-Requested-With: com.datingpro.dolly
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en,en-US;q=0.9
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Cross-Origin-Resource-Policy: cross-origin
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="static-on-bigtable"
Report-To: {"group":"static-on-bigtable","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/static-on-bigtable"}]}
Content-Length: 1150
X-Content-Type-Options: nosniff
Server: sffe
X-Xss-Protection: 0
Date: Fri, 22 Nov 2024 20:45:52 GMT
Expires: Sat, 22 Nov 2025 20:45:52 GMT
Cache-Control: public, max-age=31536000
Last-Modified: Thu, 03 Oct 2019 10:15:00 GMT
Content-Type: image/x-icon
Vary: Accept-Encoding
Age: 550151
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

..... .h.......(..... ..... .....|...O...E...M.....Ix..4z..?|..@|..
<{..Az....._.....|.....1v..;...?...>}..>z..Cy.....
...[SNIP]...
```

5.6. https://googleads.g.doubleclick.net/getconfig/pubsetting

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://googleads.g.doubleclick.net**

Path: **/getconfig/pubsetting**

Request

```
GET /getconfig/pubsetting?
app_name=com.datingpro.dolly&vnm=102&eid=318502753%2C318515867%2C318516088%2C318516381%2C318516383&js
=afma-sdk-a-v243799999.231004000.1&client=ca-app-pub-2489227358200851&admob_appcc=5341356166 HTTP/2
Host: googleads.g.doubleclick.net
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like
Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v243799999.231004000.1)
Accept: */*
X-Requested-With: com.datingpro.dolly
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en,en-US;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR
IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
Access-Control-Allow-Origin: https://googleads.g.doubleclick.net
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Date: Fri, 29 Nov 2024 05:35:05 GMT
Server: cafe
Content-Length: 337
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{"status":1,"app_id":"ca-app-pub-2489227358200851~5341356166","auto_collect_location":true,"exp_param":{"loeid":
[44766145]},"publisher_permissions":[{"platform":"ADMOB","eoid_enabled":true,"same_app_k
...[SNIP]...
```

5.7. https://googleads.g.doubleclick.net/mads/gma

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://googleads.g.doubleclick.net**

Path: **/mads/gma**

Request

```
GET /mads/gma?submodel=sdk_gphone_x86&adid_p=1&format=411x64_as&omid_v=a.1.4.14-
google_20240908&client_purpose_one=false&dv=243799205&ev=22.1.0&hl=en&js=afma-sdk-a-
v243799999.231004000.1&lv=231004600&ms=CpgECoACRfjsdkLkM3pvTf543j95aNwA_FsZktWJnMGbuy4RHmqQHAKu7q9cYr-
84IlnXgHEpag1de8BFoOYVUyxEqQIlkDleM0n1pDXK60h0vhh8IcVRnF6MGQ1wtF09YDNnykS3RWAUnPqmFKeofXkIVb4a2Bi
v40YMeMt8YQ27xb7w7gPbXMAFm0DTvv8ricGcZS523bj86jnGvqcsvhoQrlvBOJsq_-kBBbYk102jXcO7Ixc73lyAjUvH-
F8c0CW8UbEXvLBwSyxFwr95CXQcUcxo0XC1eQNai3rf3NUdHKMsHvxKXg2Eh8Ta3nwJokw7Hg-
7OtsxvHwAkMflepJ9CsROgqAAk5IfGAFarilunPo8iLCG2QAP2u-sEEYvIeXVJuaXa-K-
C6UeTdI9A9ayYuhlLzQZzuUO2In6gTOLZmvziPlMRgq0oB_-
lOYlujNGTOCt4q3CKDliUkNzSHoNr28tTumLYUliBGlvBuhYAJb_Vemej53ZSOgKpg-
gmXo2u62iYhSt1ecaTnlCr7iMoMVRQHVNK13ECdk_UnJCwVYAwjXCGiCKfT49mQ6wErmPEirymaB1dAZXUuT7QhXr0CFkYS
CbxN3caZOAcVkSdBRQ2v51qdlZhySY2635ktb3KSBlOPi-
c0b4pwqYGakOy6HBbSDoqAGgfjDZ8OUjg_vJWrawBMSECFDYWgA8SZoY0V5Xjb9G8ASlQIKgAKcbxwiCC3G8WEHWELnGvu-
wPzwmbokMHPjla_aUh5v9akoAtjrmT9Z4NoHHCwhNZT_OX53pOTYKCClLpkAHURYJ71mMUPK7tpQK9vAd_8GK491QeDer
FRk2k6eOPAhmrd6jh7m6QqYGoDNQGjTvqy05atheLzUxQnLEgCYiRW5KjmRjtWmY_hIxK8S-n_sNXC-
BfvJJdLnZf_4GRJ2RXtn7r0xsBL_jRri9dGk7iKhyRxZt-qXqrj2dq5TeeNh-
JIa3BerWTAO50mrmpyKGN10hYAoVXoNtK_jzqoWK3Cu0T9xeNrKU1k0eUrk454mx8HP4PFOa_gy9XAE9wjb0ec9EhA5DX8SsA0J-
NjRzaSUuUmd&mv=84371920.com.android.vending&lft=0&vnm=3.5.7&risd=1&u_sd=2.625&request_id=420502311&rafmt=102&target_api=34&carrier=310260&fbs_aeid=-6234431077831155454&fbs_aiid=e2f6cf45cddfbfd5703631a763303552&seq_num=2&eid=318502753%2C318515867%2C318516088%2C318516381%2C318516383&guci=0.0.0.0.0.0.0.0&adtest=on&sdk_apis=7%2C8&omid_p=Google%2Fafma-sdk-a-
v243799999.231004000.1&u_w=412&u_h=684&msid=com.datingpro.dolly&an=102.android.com.datingpro.dolly&u_audio=4&net=wi&u_so=p&preqs_in_session=1&preqs=1&time_in_session=80&sst=1732858500000&output=html&region=mobile_app&u_tz=-300&client=ca-app-pub-
2489227358200851&slotname=1852091734&gsb=wi&apm_app_id=1%3A20824395699%3Aandroid%3A9d3ef0a0146f0e1a6fc5c6&gmp_app_id=1%3A20824395699%3Aandroid%3A9d3ef0a0146f0e1a6fc5c6&apm_app_type=1&lite=0&stbg=1&caps=inlineVideo_interactiveVideo_mraid1_mraid2_mraid3_sdkVideo_exo3_th_autoplay_mediation_scroll_av_transparentBackground_sdkAdmobApiForAds_di_aso_sfv_dinm_dim_nav_navc_dinmo_ipdof_gls_xSeconds&bisch=false&blev=1&canm=false&_mv=84371920.com.android.vending&heap_free=7533165&heap_max=536870912&heap_total=25194957&wv_count=1&rdps=4250&is_lat=false&rdidl=36&idtypel=4&blob=ABPQqLE0W9yupJOE0QEyW0e4sB7CVo-
Jp1UgY2fXJXhYRSlsjCgwxXhvUaNh7v2Ed5ktOe5vx3KAhxTgr-acu8TohTYfJ7lEbp-
wOZJPQJs00ZinyvDgwZXuhoS9afd8K8GW8cUULPGV-
60xmRz0lIeRDyFl8epkW7djgMcJlI1xh5XRggCO_M0sfFpUajnDH_DFBwElL9pjNKgKAk-
Dwv6rC6PQQBv2iqasOj2iQ76XUpyg_sX5Ycs1ixHi39pEqALLE5Wa2W42LcoIYIzRuavAFxVjQeNhQANXbjgiGg5c64rXartnU3o0FNUTwQ&adk=2603848924&jsv=sdk_20190107_RC02-production-sdk_20241114_RC00 HTTP/1.1
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
x-afma-drt-cookie: DSID=ACZUy1zwTN84O6zJ6lonI7a-
FS1CTlrBElr2Q_aBHCwYD_SlA9NpfUwgQNcxj0ArOoDz4NbGcUfQGn0-VzDHbPVdBVlGvHAPlJ75MLpaCHGbRlgtUx_OBfE
x-afma-drt-v2-cookie:
CoIBCnxEU0lEPUFDWlV5MXp3VE44NE82eko2bG9ubDdhLUZTMUNUbHJCRWxyMlFfYUJIQ3dZRF9TbEE5TnBmVXdnUU5jeGowQXJPb0R6NE5iR2NVZlFHbjAtVnpESGJQVmRCVmxHdkhBUElKNzVNTHBhQ0hHYlJsZ3RVeF9PQmZFEAEYAQ==
Host: googleads.g.doubleclick.net
Connection: Keep-Alive
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Afma-Analytics-Personalization: true
X-Afma-Content-Vertical-Opted-Out: true
X-Afma-Content-Url-Opted-Out: true
```

```
X-Afma-Use-Https: false
X-Afma-Gws-Query-Id: o1JJZ67mN9-zoPMP-8DW6Q4
X-Afma-Mediation: true
Cache-Control: private, no-cache, no-store
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Date: Fri, 29 Nov 2024 05:35:32 GMT
Server: cafe
Content-Length: 131799
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{"ad_type":"banner","qdata":"x","ad_networks":[{"ad":
{"ad_base_url":"https://googleads.g.doubleclick.net","ad_html":"\u003c!DOCTYPE html\u003e\u003chtml
lang=en\u003e\u003chead\u003e\u003cmeta charset
...[SNIP]...
```

5.8. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html**

Request

```
GET /mads/static/mad/sdk/native/production/sdk-core-v40-impl.html HTTP/2
Host: googleads.g.doubleclick.net
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v243799999.231004000.1)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
X-Requested-With: com.datingpro.dolly
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en,en-US;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Content-Type-Options: nosniff
Server: cafe
```

```
Content-Length: 387132
X-Xss-Protection: 0
Date: Fri, 29 Nov 2024 05:23:43 GMT
Expires: Sat, 30 Nov 2024 05:23:43 GMT
Cache-Control: public, max-age=86400
Age: 679
Etag: 4395789294679574262
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

<!DOCTYPE html>
<html>
<head>
<script>
(function (){ /*

Copyright The Closure Library Authors.
SPDX-License-Identifier: Apache-2.0
*/
/*

Copyright 2011 Google Inc. All rights reserved.
Lic
...[SNIP]...
```

5.9. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js**

Request

```
GET /mads/static/mad/sdk/native/production/sdk-core-v40-impl.js?n=true&lv=sdk_20190107_RC02 HTTP/2
Host: googleads.g.doubleclick.net
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
Accept: */*
X-Requested-With: com.google.android.gms
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR
IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Server: cafe
Content-Length: 537947
X-Xss-Protection: 0
Date: Fri, 29 Nov 2024 02:02:38 GMT
Expires: Fri, 29 Nov 2024 06:02:38 GMT
Cache-Control: public, max-age=14400
Age: 12747
Etag: 9673142243471861567
Content-Type: text/javascript; charset=UTF-8
Vary: Accept-Encoding
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

(function (){ /*

Copyright The Closure Library Authors.
SPDX-License-Identifier: Apache-2.0
*/
/*

Copyright 2011 Google Inc. All rights reserved.
Licensed under the Apache License, Versi
...[SNIP]...
```

5.10. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.appcache

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/static/mad/sdk/native/sdk-core-v40-loader.appcache**

Request

```
GET /mads/static/mad/sdk/native/sdk-core-v40-loader.appcache HTTP/2
Host: googleads.g.doubleclick.net
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like
Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
Accept: */*
X-Requested-With: com.google.android.gms
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Content-Type-Options: nosniff
Server: cafe
Content-Length: 192
X-Xss-Protection: 0
Date: Fri, 29 Nov 2024 05:25:49 GMT
Expires: Fri, 29 Nov 2024 07:25:49 GMT
Cache-Control: public, max-age=7200
Age: 582
Etag: 16027413122022871166
Content-Type: text/cache-manifest; charset=UTF-8
Vary: Accept-Encoding
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

CACHE MANIFEST
/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js

NETWORK:
*

# AppCache versioning info below:
# pid = 0e1c42b3-e0ba-4b09-b3b8-99192dc8b2ad
# cn = sdk_20241120_RC00
```

5.11. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/static/mad/sdk/native/sdk-core-v40-loader.html**

Request

```
GET /mads/static/mad/sdk/native/sdk-core-v40-loader.html HTTP/2
Host: googleads.g.doubleclick.net
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
X-Requested-With: com.google.android.gms
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
```

```
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
Vary: Accept-Encoding
Date: Fri, 29 Nov 2024 05:35:05 GMT
Expires: Fri, 29 Nov 2024 05:35:05 GMT
Cache-Control: private, max-age=86400
Content-Type: text/html; charset=UTF-8
Etag: 16295587571342835724
X-Content-Type-Options: nosniff
Server: cafe
Content-Length: 196
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000


<!DOCTYPE html>
<html>
<head>
<script>
var efs = false;
</script>
<script src="/mads/static/mad/sdk/native/sdk-core-v40-loader.js"></script>
</head>
<body></body>
</html>
```

5.12. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/static/mad/sdk/native/sdk-core-v40-loader.js**

Request

```
GET /mads/static/mad/sdk/native/sdk-core-v40-loader.js HTTP/2
Host: googleads.g.doubleclick.net
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
Accept: */*
X-Requested-With: com.google.android.gms
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
```

```
Referer: https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR
IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Server: cafe
Content-Length: 47613
X-Xss-Protection: 0
Date: Fri, 29 Nov 2024 04:47:09 GMT
Expires: Fri, 29 Nov 2024 08:47:09 GMT
Cache-Control: public, max-age=14400
Age: 2876
Etag: 11080626372616993405
Content-Type: text/javascript; charset=UTF-8
Vary: Accept-Encoding
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

// Copyright 2013 Google Inc. All Rights Reserved.
(function(){var aa="DOMContentLoaded",ba="Storage mechanism: Invalid value was encountered",ca="Storage: Invalid value
was encountered",da="canary-ex
...[SNIP]...
```

---

6. Email addresses disclosed

There are 4 instances of this issue:

- https://googleads.g.doubleclick.net/mads/gma
- https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html
- https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js
- https://www.deliverizate.es/api/userNearByMePageFilters

Issue background

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Issue remediation

Consider removing any email addresses that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as helpdesk@example.com).

To reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-200: Information Exposure
- CAPEC-37: Retrieve Embedded Sensitive Data

6.1. https://googleads.g.doubleclick.net/mads/gma

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/gma**

Issue detail

The following email address was disclosed in the response:

- robert@broofa.com

Request

GET /mads/gma?submodel=sdk_gphone_x86&adid_p=1&format=411x64_as&omid_v=a.1.4.14-google_20240908&client_purpose_one=false&dv=243799205&ev=22.1.0&hl=en&js=afma-sdk-a-v243799999.231004000.1&lv=231004600&ms=CpgECoACRfjsdkLkM3pvTf543j95aNwA_FsZktWJnMGbuy4RHmqQHAKu7q9cYr-84IlnXgHEpag1de8BFoOYVUyxEqQIlkDleM0n1pDXK60h0vhh8IcVRnF6MGQ1wtF09YDNnykS3RWAUnPqmFKeofXkIVb4a2Biv40YMeMt8YQ27xb7w7gPbXMAFm0DTvv8ricGcZS523bj86jnGvqcsvhoQrlvBOJsq_-kBBbYk102jXcO7Ixc73lyAjUvH-F8c0CW8UbEXvLBwSyxFwr95CXQcUcxo0XC1eQNai3rf3NUdHKMsHvxKXg2Eh8Ta3nwJokw7Hg-7OtsxvHwAkMflepJ9CsROgqAAk5IfGAFarilunPo8iLCG2QAP2u-sEEYvIeXVJuaXa-K-C6UeTdI9A9ayYuhlLzQZzuUO2In6gTOLZmvziPlMRgq0oB_-IOYlujNGTOCt4q3CKDliUkNzSHoNr28tTumLYUliBGlvBuhYAJb_Vemej53ZSOgKpg-gmXo2u62iYhSt1ecaTnlCr7iMoMVRQHVNK13ECdk_UnJCwVYAwjXCGiCKfT49mQ6wErmPEirymaB1dAZXUuT7QhXr0CFkYSCbxN3caZOAcVkSdBRQ2v51qdlZhySY2635ktb3KSBlOPi-c0b4pwqYGakOy6HBbSDoqAGgfjDZ8OUjg_vJWrawBMSECFDYWgA8SZoY0V5Xjb9G8ASlQIKgAKcbxwiCC3G8WEHWELnGvu-wPzwmbokMHPjla_aUh5v9akoAtjrmT9Z4NoHHCwhNZT_OX53pOTYKCClLpkAHURYJ71mMUPK7tpQK9vAd_8GK491QeDerFRk2k6eOPAhmrd6jh7m6QqYGoDNQGjTvqy05atheLzUxQnLEgCYiRW5KjmRjtWmY_hIxK8S-n_sNXC-BfvJJdLnZf_4GRJ2RXtn7r0xsBL_jRri9dGk7iKhyRxZt-qXqrj2dq5TeeNh-JIa3BerWTAO50mrmpyKGN10hYAoVXoNtK_jzqoWK3Cu0T9xeNrKU1k0eUrk454mx8HP4PFOa_gy9XAE9wjb0ec9EhA5DX8SsA0J-NjRzaSUuUmd&mv=84371920.com.android.vending&lft=0&vnm=3.5.7&risd=1&u_sd=2.625&request_id=420502311&rafmt=102&target_api=34&carrier=310260&fbs_aeid=-6234431077831155454&fbs_aiid=e2f6cf45cddfbfd5703631a763303552&seq_num=2&eid=318502753%2C318515867%2C318516088%2C318516381%2C318516383&guci=0.0.0.0.0.0.0.0&adtest=on&sdk_apis=7%2C8&omid_p=Google%2Fafma-sdk-a-v243799999.231004000.1&u_w=412&u_h=684&msid=com.datingpro.dolly&an=102.android.com.datingpro.dolly&u_audio=4&net=wi&u_so=p&preqs_in_session=1&preqs=1&time_in_session=80&sst=1732858500000&output=html&region=mobile_app&u_tz=-300&client=ca-app-pub-2489227358200851&slotname=1852091734&gsb=wi&apm_app_id=1%3A20824395699%3Aandroid%3A9d3ef0a0146f0e1a6fc

```
5c6&gmp_app_id=1%3A20824395699%3Aandroid%3A9d3ef0a0146f0e1a6fc5c6&apm_app_type=1&lite=0&stbg=1&caps=inlineVideo_interactiveVideo_mraid1_mraid2_mraid3_sdkVideo_exo3_th_autoplay_mediation_scroll_av_transparentBackground_sdkAdmobApiForAds_di_aso_sfv_dinm_dim_nav_navc_dinmo_ipdof_gls_xSeconds&bisch=false&blev=1&canm=false&_mv=84371920.com.android.vending&heap_free=7533165&heap_max=536870912&heap_total=25194957&wv_count=1&rdps=4250&is_lat=false&rdidl=36&idtypel=4&blob=ABPQqLE0W9yupJOE0QEyW0e4sB7CVo-Jp1UgY2fXJXhYRSlsjCgwxXhvUaNh7v2Ed5ktOe5vx3KAhxTgr-acu8TohTYfJ7lEbp-wOZJPQJs00ZinyvDgwZXuhoS9afd8K8GW8cUULPGV-60xmRz0lIeRDyFl8epkW7djgMcJll1xh5XRggCO_M0sfFpUajnDH_DFBwElL9pjNKgKAk-Dwv6rC6PQQBv2iqasOj2iQ76XUpyg_sX5Ycs1ixHi39pEqALLE5Wa2W42LcoIYIzRuavAFxVjQeNhQANXbjgiGg5c64rXartnU3o0FNUTwQ&adk=2603848924&jsv=sdk_20190107_RC02-production-sdk_20241114_RC00 HTTP/1.1
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
x-afma-drt-cookie: DSID=ACZUy1zwTN84O6zJ6lonl7a-FS1CTlrBElr2Q_aBHCwYD_SlA9NpfUwgQNcxj0ArOoDz4NbGcUfQGn0-VzDHbPVdBVlGvHAPIJ75MLpaCHGbRlgtUx_OBfE
x-afma-drt-v2-cookie: CoIBCnxEU0lEPUFDWlV5MXp3VE44NE82eko2bG9ubDdhLUZTMUNUbHJCRWxyMlFfYUJIQ3dZRF9TbEE5TnBmVXdnUU5jeGowQXJPb0R6NE5iR2NVZlFHbjAtVnpESGJQVmRCVmxHdkhBUElKNzVNTHBhQ0hHYlJsZ3RVeF9PQmZFEAEYAQ==
Host: googleads.g.doubleclick.net
Connection: Keep-Alive
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Afma-Analytics-Personalization: true
X-Afma-Content-Vertical-Opted-Out: true
X-Afma-Content-Url-Opted-Out: true
X-Afma-Use-Https: false
X-Afma-Gws-Query-Id: o1JJZ67mN9-zoPMP-8DW6Q4
X-Afma-Mediation: true
Cache-Control: private, no-cache, no-store
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Date: Fri, 29 Nov 2024 05:35:32 GMT
Server: cafe
Content-Length: 131799
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{"ad_type":"banner","qdata":"x","ad_networks":[{"ad":{"ad_base_url":"https://googleads.g.doubleclick.net","ad_html":"\u003c!DOCTYPE html\u003e\u003chtml lang=en\u003e\u003chead\u003e\u003cmeta charset
...[SNIP]...
d.constructor===Object\u0026\u0026(d=Object.entries(d));Array.isArray(d)?d.forEach(function(h){return e(h[1],h[0])}):d.forEach(e);return Fa(a+b+c)};/* Math.uuid.js (v1.4) http://www.broofa.com mailto:robert@broofa.com Copyright (c) 2010 Robert Kieffer Dual licensed under the MIT and GPL licenses. */ var Ka=\"0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz\".split(\"\");function La(a){for(var b=Array(
...[SNIP]...
```

6.2. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html**

Issue detail

The following email address was disclosed in the response:

- robert@broofa.com

Request

```
GET /mads/static/mad/sdk/native/production/sdk-core-v40-impl.html HTTP/2
Host: googleads.g.doubleclick.net
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v243799999.231004000.1)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
X-Requested-With: com.datingpro.dolly
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en,en-US;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Content-Type-Options: nosniff
Server: cafe
Content-Length: 387132
X-Xss-Protection: 0
Date: Fri, 29 Nov 2024 05:23:43 GMT
Expires: Sat, 30 Nov 2024 05:23:43 GMT
Cache-Control: public, max-age=86400
Age: 679
Etag: 4395789294679574262
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

<!DOCTYPE html>
<html>
<head>
<script>
(function (){ /*

Copyright The Closure Library Authors.
SPDX-License-Identifier: Apache-2.0
*/
```

```
/*

Copyright 2011 Google Inc. All rights reserved.
Lic
...[SNIP]...
g[b];return a instanceof Array?a:c},kD=function(a,b){b&&Object.assign(a.g,b)},lD=function(a,b){b&&
(a.g=b)};fD.prototype.reset=function(){this.g={}};/*

Math.uuid.js (v1.4)
http://www.broofa.com
mailto:robert@broofa.com
Copyright (c) 2010 Robert Kieffer
Dual licensed under the MIT and GPL licenses.
*/
var mD="0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz".split(""),nD=function(){var a=
[],b;a[8]=a[13]
...[SNIP]...
```

6.3. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js**

Issue detail

The following email address was disclosed in the response:

- robert@broofa.com

Request

```
GET /mads/static/mad/sdk/native/production/sdk-core-v40-impl.js?n=true&lv=sdk_20190107_RC02 HTTP/2
Host: googleads.g.doubleclick.net
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like
Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
Accept: */*
X-Requested-With: com.google.android.gms
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR
IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
```

```
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Server: cafe
Content-Length: 537947
X-Xss-Protection: 0
Date: Fri, 29 Nov 2024 02:02:38 GMT
Expires: Fri, 29 Nov 2024 06:02:38 GMT
Cache-Control: public, max-age=14400
Age: 12747
Etag: 9673142243471861567
Content-Type: text/javascript; charset=UTF-8
Vary: Accept-Encoding
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

(function (){ /*

Copyright The Closure Library Authors.
SPDX-License-Identifier: Apache-2.0
*/
/*

Copyright 2011 Google Inc. All rights reserved.
Licensed under the Apache License, Versi
...[SNIP]...
;return a instanceof Array?a:c},kD=function(a,b){b&&Object.assign(a.g,b)},lD=function(a,b){b&&
(a.g=b)};fD.prototype.reset=function(){this.g={}};/*

Math.uuid.js (v1.4)
http://www.broofa.com
mailto:robert@broofa.com
Copyright (c) 2010 Robert Kieffer
Dual licensed under the MIT and GPL licenses.
*/
var mD="0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz".split(""),nD=function(){var a=
[],b;a[8]=a
...[SNIP]...
```

6.4. https://www.deliverizate.es/api/userNearByMePageFilters

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://www.deliverizate.es**
Path:	**/api/userNearByMePageFilters**

Issue detail

The following email address was disclosed in the response:

- Msampson147@gmail.com

Request

```
POST /api/userNearByMePageFilters HTTP/1.1
Host: www.deliverizate.es
Content-Type: application/json;
Content-Length: 686
Accept-Encoding: gzip, deflate, br
User-Agent: okhttp/5.0.0-alpha.2
Connection: keep-alive

{"fb_id":"10175433816400387396 7","lat_long":"37.4219983,
-122.084","gender":"1","relationship":"","distance":"10000","device_token":"fcklSmKVSiiHSvndvXr01v:APA91bHiiA44QHJmtuSR
DrwRWqvhQs-QfJiytLnU56O4
...[SNIP]...
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 29 Nov 2024 05:35:02 GMT
Server: Apache/2.4.52 (Ubuntu)
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 55
Access-Control-Allow-Origin: *
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json
Content-Length: 31098

{"code":"200","page":1,"page_limit":9,"msg":
[{"fb_id":"12533396944","first_name":"Cass","last_name":"","birthday":"20","about_me":"","audio":"","audio_prompt":"","distance"
:"676 miles away","km":676,"
...[SNIP]...
County,United States","language":"en","preferences":null,"promoted":0,"last_active":"2024-09-13
03:46:42","swipe":"false","match":"false","isnew":"yes","block":0},
{"fb_id":"14807728308","first_name":"Msampson147@gmail.com","last_name":"","birthday":"40","about_me":"","audio":"","audio
_prompt":"","distance":"645 miles
away","km":645,"gender":"1","image1":"https:\/\/www.deliverizate.es\/storage\/mainimage\/17241961502024
...[SNIP]...
```

---

7. Cacheable HTTPS response

There are 8 instances of this issue:

- https://dl.google.com/vision/1/creditcard/gocr_credit_card_ocr_v0.zip
- https://geomobileservices-pa.googleapis.com/google.internal.maps.geomobileservices.geocoding.v3mobile.GeocodingService/ReverseGeocode
- https://gmscompliance-pa.googleapis.com/google.internal.gmscore.gmscompliance.v1.GmsCompliance/GetEnforcement
- https://googleads.g.doubleclick.net/getconfig/pubsetting
- https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/native_ads.html
- https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html
- https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.appcache
- https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html

Issue description

Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Issue remediation

Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:

- Cache-control: no-store
- Pragma: no-cache

References

- Web Security Academy: Information disclosure

Vulnerability classifications

- CWE-524: Information Exposure Through Caching
- CWE-525: Information Exposure Through Browser Caching
- CAPEC-37: Retrieve Embedded Sensitive Data

7.1. https://dl.google.com/vision/1/creditcard/gocr_credit_card_ocr_v0.zip

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://dl.google.com**
Path:	**/vision/1/creditcard/gocr_credit_card_ocr_v0.zip**

Request

```
GET /vision/1/creditcard/gocr_credit_card_ocr_v0.zip HTTP/2
Host: dl.google.com
User-Agent: com.google.android.gms/244534025 (Linux; U; Android 11; en_US; sdk_gphone_x86; Build/RSR1.201013.001; Cronet/132.0.6779.0)
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Accept-Ranges: bytes
Content-Disposition: attachment
Content-Security-Policy: default-src 'none'
Server: downloads
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 0
Date: Fri, 29 Nov 2024 05:35:31 GMT
Cache-Control: public,max-age=86400
```

```
Last-Modified: Fri, 21 Oct 2022 23:56:48 GMT
Etag: "fd7fee"
Content-Type: application/zip
Content-Length: 696543
Age: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

PK.....!()(x.............credit_card_ocr_engine.binarypb.T]k.A.e..uj?..b..].-E..M.m@..m.4M.)(.....]..Yfg.....D.....?A_|.._..n..h>...
{..s.=w.....].[...I...|A.^    8.....9/b..I.H..+;.....&-.f.!
...[SNIP]...
```

7.2. https://geomobileservices-pa.googleapis.com/google.internal.maps.geomobileservices.geocoding.v3mobile.GeocodingService/ReverseGeocode

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://geomobileservices-pa.googleapis.com**
Path:	**/google.internal.maps.geomobileservices.geocoding.v3mobile.GeocodingService/ReverseGeocode**

Request

```
POST /google.internal.maps.geomobileservices.geocoding.v3mobile.GeocodingService/ReverseGeocode HTTP/1.1
Host: geomobileservices-pa.googleapis.com
User-Agent: com.google.android.gms/244534025 (Linux; U; Android 11; en_US; sdk_gphone_x86; Build/RSR1.201013.001;
Cronet/132.0.6779.0) grpc-java-cronet/1.69.0-SNAPSHOT
Content-Type: application/grpc
Te: trailers
X-Goog-Spatula:
CjYKFmNvbS5nb29nbGUuYW5kcm9pZC5nbXMaHE9KR0tSVDBIR1pOVStMR2E4RjdHVml6dFY0Zz0Y8M6FupvDrb04
Grpc-Accept-Encoding: gzip
Grpc-Timeout: 9952874u
Content-Length: 52
Connection: keep-alive

..../
.    *}....B@..=..`.^...en0.:.com.datingpro.dolly
```

Response

```
HTTP/2 200 OK
Content-Disposition: attachment
Content-Type: application/grpc
Date: Fri, 29 Nov 2024 05:35:00 GMT
Server-Timing: gfet4t7; dur=29
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Grpc-Status: 0
Content-Disposition: attachment

.....
..
...FGoogle Building 43, 43 Amphitheatre Pkwy, Mountain View, CA 94043, USA.+
....Google Building 43..Google Building 43..
```

."..43..43.,
....Amphitheatre Parkway..Amphitheatre Pkwy."
....Mount
...[SNIP]...

7.3. https://gmscompliance-pa.googleapis.com/google.internal.gmscore.gmscompliance.v1.GmsCompliance/GetEnforcement

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://gmscompliance-pa.googleapis.com**
Path:	**/google.internal.gmscore.gmscompliance.v1.GmsCompliance/GetEnforcement**

Request

```
POST /google.internal.gmscore.gmscompliance.v1.GmsCompliance/GetEnforcement HTTP/2
Host: gmscompliance-pa.googleapis.com:443
User-Agent: grpc-java-okhttp/1.69.0-SNAPSHOT
Content-Type: application/grpc
Te: trailers
X-Goog-Api-Key: AIzaSyAP-gfH3qvi6vgHZbSYwQ_XHqV_mXHhzIk
X-Android-Package: com.google.android.gms
X-Android-Cert: 38918A453D07199354F8B19AF05EC6562CED5788
Grpc-Accept-Encoding: gzip
Grpc-Timeout: 59908669u
Content-Length: 8212

... .

.........8...
Rgoogle/sdk_gphone_x86/generic_x86_arm:11/RSR1.201013.001/6903271:user/release-
keys..google..sdk_gphone_x86".generic_x86_arm*.Google2.sdk_gphone_x86:.@.JRgoogle/sdk_gphone_x86/gen
...[SNIP]...
```

Response

```
HTTP/2 200 OK
Content-Type: application/grpc
Grpc-Accept-Encoding: identity, deflate, gzip
Content-Disposition: attachment
Date: Fri, 29 Nov 2024 05:33:35 GMT
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Grpc-Status: 0
Endpoint-Load-Metrics-Bin: MeTOEIDQIzBASY9MYzs/e9A/
Grpc-Server-Stats-Bin: AACx+bYCAAAAAA
Pc-High-Bwd-Bin: S2dJWUN3

....c
....................."
.........8*..
Rgoogle/sdk_gphone_x86/generic_x86_arm:11/RSR1.201013.001/6903271:user/release-
```

keys..google..sdk_gphone_x86".generic_x86_arm*.Google2.sdk_gphone_x86:.@.JRgoog
...[SNIP]...

7.4. https://googleads.g.doubleclick.net/getconfig/pubsetting

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/getconfig/pubsetting**

Request

```
GET /getconfig/pubsetting?
app_name=com.datingpro.dolly&vnm=102&eid=318502753%2C318515867%2C318516088%2C318516381%2C318516383&js
=afma-sdk-a-v243799999.231004000.1&client=ca-app-pub-2489227358200851&admob_appcc=5341356166 HTTP/2
Host: googleads.g.doubleclick.net
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like
Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v243799999.231004000.1)
Accept: */*
X-Requested-With: com.datingpro.dolly
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en,en-US;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR
IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
Access-Control-Allow-Origin: https://googleads.g.doubleclick.net
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Date: Fri, 29 Nov 2024 05:35:05 GMT
Server: cafe
Content-Length: 337
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{"status":1,"app_id":"ca-app-pub-2489227358200851~5341356166","auto_collect_location":true,"exp_param":{"loeid":
[44766145]},"publisher_permissions":[{"platform":"ADMOB","eoid_enabled":true,"same_app_k
...[SNIP]...
```

7.5. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/native_ads.html

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/static/mad/sdk/native/native_ads.html**

Request

```
GET /mads/static/mad/sdk/native/native_ads.html HTTP/2
Host: googleads.g.doubleclick.net
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v243799999.231004000.1)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
X-Requested-With: com.datingpro.dolly
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en,en-US;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Content-Type-Options: nosniff
Server: cafe
Content-Length: 172221
X-Xss-Protection: 0
Date: Fri, 29 Nov 2024 02:17:49 GMT
Expires: Fri, 29 Nov 2024 06:17:49 GMT
Cache-Control: public, max-age=14400
Age: 11947
Etag: 1867019947228510267
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

<!DOCTYPE html>
<html>
<head>
<script>
(function (){ /*

Copyright The Closure Library Authors.
SPDX-License-Identifier: Apache-2.0
```

```
*/
/*

Copyright Google LLC
SPDX-License-Identifier: Apach
...[SNIP]...
```

7.6. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/static/mad/sdk/native/production/sdk-core-v40-impl.html**

Request

```
GET /mads/static/mad/sdk/native/production/sdk-core-v40-impl.html HTTP/2
Host: googleads.g.doubleclick.net
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v243799999.231004000.1)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
X-Requested-With: com.datingpro.dolly
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en,en-US;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Content-Type-Options: nosniff
Server: cafe
Content-Length: 387132
X-Xss-Protection: 0
Date: Fri, 29 Nov 2024 05:23:43 GMT
Expires: Sat, 30 Nov 2024 05:23:43 GMT
Cache-Control: public, max-age=86400
Age: 679
Etag: 4395789294679574262
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

```
<!DOCTYPE html>
<html>
<head>
<script>
(function (){ /*

Copyright The Closure Library Authors.
SPDX-License-Identifier: Apache-2.0
*/
/*

Copyright 2011 Google Inc. All rights reserved.
Lic
...[SNIP]...
```

7.7. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.appcache

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/static/mad/sdk/native/sdk-core-v40-loader.appcache**

Request

```
GET /mads/static/mad/sdk/native/sdk-core-v40-loader.appcache HTTP/2
Host: googleads.g.doubleclick.net
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
Accept: */*
X-Requested-With: com.google.android.gms
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
X-Content-Type-Options: nosniff
Server: cafe
Content-Length: 192
X-Xss-Protection: 0
Date: Fri, 29 Nov 2024 05:25:49 GMT
Expires: Fri, 29 Nov 2024 07:25:49 GMT
Cache-Control: public, max-age=7200
```

```
Age: 582
Etag: 16027413122022871166
Content-Type: text/cache-manifest; charset=UTF-8
Vary: Accept-Encoding
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

CACHE MANIFEST
/mads/static/mad/sdk/native/production/sdk-core-v40-impl.js

NETWORK:
*

# AppCache versioning info below:
# pid = 0e1c42b3-e0ba-4b09-b3b8-99192dc8b2ad
# cn = sdk_20241120_RC00
```

7.8. https://googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.html

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://googleads.g.doubleclick.net**
Path:	**/mads/static/mad/sdk/native/sdk-core-v40-loader.html**

Request

```
GET /mads/static/mad/sdk/native/sdk-core-v40-loader.html HTTP/2
Host: googleads.g.doubleclick.net
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36 (Mobile; afma-sdk-a-v244534025.244534025.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
X-Requested-With: com.google.android.gms
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
P3p: policyref="https://googleads.g.doubleclick.net/pagead/gcn_p3p_.xml", CP="CURa ADMa DEVa TAIo PSAo PSDo OUR IND UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR"
Timing-Allow-Origin: *
Cross-Origin-Resource-Policy: cross-origin
Vary: Accept-Encoding
Date: Fri, 29 Nov 2024 05:35:05 GMT
Expires: Fri, 29 Nov 2024 05:35:05 GMT
Cache-Control: private, max-age=86400
```

```
Content-Type: text/html; charset=UTF-8
Etag: 16295587571342835724
X-Content-Type-Options: nosniff
Server: cafe
Content-Length: 196
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000


<!DOCTYPE html>
<html>
<head>
<script>
var efs = false;
</script>
<script src="/mads/static/mad/sdk/native/sdk-core-v40-loader.js"></script>
</head>
<body></body>
</html>
```

---

8. Base64-encoded data in parameter

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://graph.facebook.com**
Path:	**/network_ads_common**

Issue detail

The following parameter appears to contain Base64-encoded data:

- **M_BANNER_KEY = com.datingpro.dolly com.android.vending**

Issue background

Applications sometimes Base64-encode parameters in an attempt to obfuscate them from users or facilitate transport of binary data. The presence of Base64-encoded data may indicate security-sensitive information or functionality that is worthy of further investigation. The data should be reviewed to determine whether it contains any interesting information, or provides any additional entry points for malicious input.

Vulnerability classifications

- CWE-310: Cryptographic Issues
- CWE-311: Missing Encryption of Sensitive Data
- CAPEC-37: Retrieve Embedded Sensitive Data

Request

```
POST /network_ads_common HTTP/1.1
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Accept-Charset: UTF-8
X-FB-Pool-Routing-Token:
eJx9VVtvm0oQ/ivIT61k493l6uZpbbCDgsECnJyoHK24LC4KMRbGaZKq/72zi5PUOj31A9qdb+bbufvHiG42863nO6MvI4zIaIDzyH
```

```
Lagi2uXJTFbx0JsacQ2bAMh0zBBYQEmrsM8R4Bf/wXJLfU3NKJS+0c6qo+MP57S0Zd01Hcnno7G6Sg7PLBj/cqlVLctzQQ2ifT1I
39t95y1VXXkvVSYYBvJ39n2wI591vW8ZB3Pju1eKvl0G4CfEVuG28BhdOMRLPXh/ZLnp90uy5vhwSprjoMfEmBPWXMakCBN0
ymVUH6qm5L1L4dL5CcEuA285B6Ckzxwp4uFG8fe3PNBztyAzn3X+R3fbAK6dkGyLdumeQHRNY2Z+0+48em9GwEgMiM0lxu
4oKLKKo7snNs6yVBVVcSclTY3bKusTJSBYiweDAOWeJL3XBQd6SoiM8DX9EbIV227a7isUhR58iW6L7u2LgWHcwO13dDBb1
E9bayPjbE1xniMzTGGgy0K6rhBPGgQ1SSGMF1Erhuwa9dbXScgN23tTHjrRsIxIVOxpaIP5TvPSa5BrmM89FUcbqOF8NLxIneR
DARwzd49DGNBJ+LDQxrZ2gvY5TMES8WLyGhA/XA1tF/f9lnDHvlj273IShJkmTOsmaY+tFNR8IZ37SPveccGlZlqWaZ27p8OC
Pq63bNniSEV/cHub9jrGbMx0fShy4tvWber97sBGWyesroRLfq7rzOi6zMoO7n05PXitXfxy4U4z3p4fZBh9CatOs7Z8ZAV59nTbV2
ziUXQ0NoOTSjbRKFs6GDFwk0CaRbZ3Z+aRvR+DCNGV24gyr5uX+umydKpoSLlk1/vT89XyrkMCsZXyrF8YLvDNzHPz7apzM
VMpdMojrBKEEZYUxECte9PnxV6ODT8juc3dQ98mqVqpvLp5jpZ+2OlqR+4suLFQ/tZueXdEYJNp9DqyuKbSHI6tYFI1THSVIxM
Zd3mdcOVOKuyrn4n+7qc0wBm+FTWfF/wgPff2+5h2XZnh6+W81jgH7fbdApBgNk8nRbto1pCmve7Q9eqcowFAiqaaqgWnOdC
HRE43cbpdOh+uPiLdMr3YoyiMEzkXhAduw4d14fzZYYAWG6DwPXZIoxc5t5CnmM5MwiPdayb8CEWfJA8aeKkj3UYKfEh4oM+
OGAGVheLaA6b0RcT94doxNjEsJYAtfNKq6yCF9y2DV4ahOecc40TUuW6YXCj5GXJM3wFNn64oJKS7+EWuMldGN2w5H7jng
P1nCUVLhBU5dzCkzLP0EQvMJnYOeETs8jzQiv1oqzkAkySyJtvRdPBXwrYibwlS7acMzH+XhAn1P/Pdj1vCVmJ/29iyOk2SKL7j2
Z+o4vOKTlvHvWJ70vIzV+owC5xP4je1rF0ucq1kmO9mHBe4ImuV/kkMziaFJaRk9yozApbo5+/APDOH+o=
user-agent: Mozilla/5.0 (Linux; Android 11; sdk_gphone_x86 Build/RSR1.201013.001; wv) AppleWebKit/537.36 (KHTML, like
Gecko) Version/4.0 Chrome/83.0.4103.106 Mobile Safari/537.36
[FBAN/AudienceNetworkForAndroid;FBSN/Android;FBSV/11;FBAB/com.datingpro.dolly;FBAV/3.5.7;FBBV/102;FBVS/6.17.0;FB
LC/en]
Host: graph.facebook.com
Connection: Keep-Alive
Accept-Encoding: gzip, deflate, br
Content-Length: 1973

COPPA=false&APPBUILD=102&ID_CACHE_TS_MS=1732858500656&KG_RESTRICTED=false&VALPARAMS=%7B%22is_e
mu%22%3A%22true%22%2C%22apk_size%22%3A%2248736065%22%2C%22timezone_offset%22%3A%22-
18000000%22%2C%22app_st
...[SNIP]...
500.696&CARRIER=Android&SDK_CAPABILITY=%5B3%2C4%2C5%2C7%2C11%2C16%2C17%2C18%5D&CLIENT_REQU
EST_ID=ec8225cd-732b-4e10-9dc3-
f2333cba1d94&DENSITY=2.625&AD_REPORTING_CONFIG_LAST_UPDATE_TIME=0&M_BANNER_KEY=Y29tLmRhdGluZ3
Byby5kb2xseSBjb20uYW5kcm9pZC52ZW5kaW5n&SCREEN_HEIGHT=683&SDK_VERSION=6.17.0&SDK=android&OSVERS
=11&ANALOG=%7B%22total_memory%22%3A%222076913664%22%2C%22accelerometer_y%22%3A%229.776321%22%2
C%22rotation_x%22%3A%220.0%22%2C%22accelerometer_x
...[SNIP]...
```

Response

```
HTTP/2 200 OK
Content-Type: text/javascript; charset=UTF-8
Vary: Origin
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Facebook-Api-Version: v16.0
Strict-Transport-Security: max-age=15552000; preload
Pragma: no-cache
Cache-Control: private, no-cache, no-store, must-revalidate
Expires: Sat, 01 Jan 2000 00:00:00 GMT
X-Fb-Request-Id: AvBYN7ZB7-DOt8YYdF8fTal
X-Fb-Trace-Id: F5dn2NDGoUr
X-Fb-Rev: 1018526344
X-Fb-Debug: HVa3KC6M+sKCCjsoKOAnI92uJ41qL5aPjYxehQtCF72lqCtkPBffDa+uQ3enGIkAztdw+1XB+Gqz7nTMVoc5tw==
Content-Length: 19882
Date: Fri, 29 Nov 2024 05:35:02 GMT
X-Fb-Connection-Quality: EXCELLENT; q=0.9, rtt=12, rtx=0, c=10, mss=1392, tbw=501, tp=-1, tpl=-1, uplat=179, ullat=0
Alt-Svc: h3=":443"; ma=86400

{
"type": "error",
"code": 1001,
"message": "No fill. We are not able to serve ads to this person. Please refer to
https://developers.facebook.com/docs/audience-network/faq#a12. If you are in
...[SNIP]...
```

9. Content type is not specified

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://tnzslk-launches.appsflyersdk.com**
Path:	**/api/v6.12/androidevent**

Issue detail

This issue was found in multiple locations under the reported path.

Issue background

If a response does not specify a content type, then the browser will usually analyze the response and attempt to determine the MIME type of its content. This can have unexpected results, and if the content contains any user-controllable data may lead to cross-site scripting or other client-side vulnerabilities.

In most cases, the absence of a content type statement does not constitute a security flaw, particularly if the response contains static content. You should review the contents of affected responses, and the context in which they appear, to determine whether any vulnerability exists.

Issue remediation

For every response containing a message body, the application should include a single Content-type header that correctly and unambiguously states the MIME type of the content in the response body.

References

- Web Security Academy: Cross-site scripting

Vulnerability classifications

- CWE-16: Configuration
- CAPEC-63: Cross-Site Scripting (XSS)

Request

```
POST /api/v6.12/androidevent?app_id=com.datingpro.dolly&buildnumber=6.12.1 HTTP/1.1
Content-Type: application/octet-stream
Content-Length: 1912
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; sdk_gphone_x86 Build/RSR1.201013.001)
Host: tnzslk-launches.appsflyersdk.com
Connection: Keep-Alive
Accept-Encoding: gzip, deflate, br

....AE-I..{Kh.\......0.w.X?....!..#@........SIZ.`M.8...W...Jd5u.3~...A..[..S.F.I.R...j.[.5iK.....#VyBO..&...)...W...g&........1...j|M....V.sa.I
   ..6...&..b..S+X=..
!....Q>vg..u...F..M......aN..r.._|..
...[SNIP]...
```

Response

```
HTTP/2 403 Forbidden
Content-Length: 9
Date: Fri, 29 Nov 2024 05:34:54 GMT
X-Cache: Error from cloudfront
Via: 1.1 5f928efc6cc9f0bbea9fe5327d80c446.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C1
X-Amz-Cf-Id: lTyFRclDh21wECDORrBiYR1UZmPDtrX2nXVBS2H15WtiZUGp2BaxLw==

forbidden
```

Report generated by Burp Suite web vulnerability scanner v2024.9.5, at Fri Nov 29 00:38:06 EST 2024.