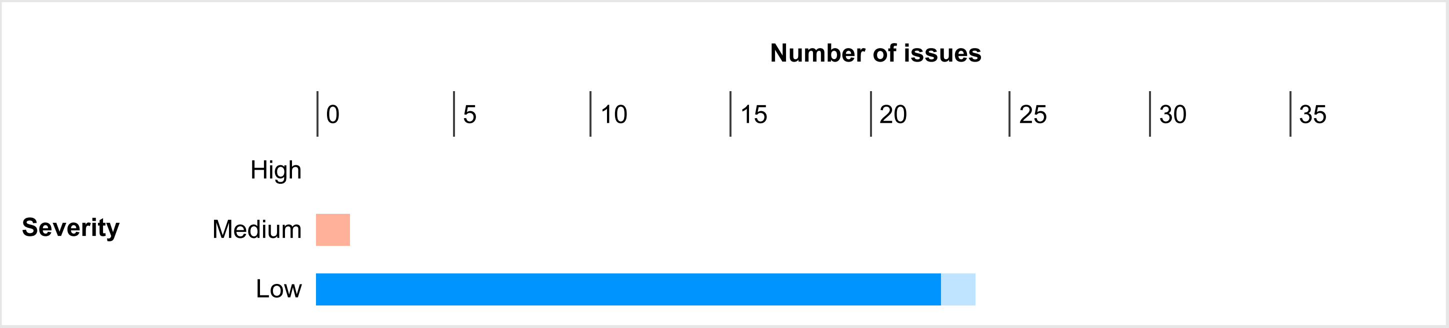
Burp Scanner Report

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
	High	0	0	0	0
	Medium	0	1	0	1
Severity	Low	19	0	1	20
	Information	35	1	0	36
	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. Session token in URL

Summary

Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://api-mobi.soundcloud.com**
Path:	**/media/soundcloud:tracks:1610873220/70e892cc-fe64-41f4-b0c6-d4ed9fb9a287/stream/hls**

Issue detail

The URL in the request appears to contain a session token within the query string:

- https://api-mobi.soundcloud.com/media/soundcloud:tracks:1610873220/70e892cc-fe64-41f4-b0c6-d4ed9fb9a287/stream/hls?secret_token=s-NVt86r3593y&client_id=KKzJxmw11tYpCs6T24P4uUYhqmjalG6M&track_authorization=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJnZW8iOiJDQSIsInN1YiI6IiIsInJpZCI6IiIsImlhdCI6MTczMjg1Njk3M30.rOb9sVq2g-xoRptLAjZvMUZNPNfLQ5b-rD7Vpgk9FNw&stage=

Issue background

Sensitive information within URLs may be logged in various locations, including the user's browser, the web server, and any forward or reverse proxy servers between the two endpoints. URLs may also be displayed on-screen, bookmarked or emailed around by users. They may be disclosed to third parties via the Referer header when any off-site links are followed. Placing session tokens into the URL increases the risk that they will be captured by an attacker.

Issue remediation

Applications should use an alternative mechanism for transmitting session tokens, such as HTTP cookies or hidden fields in forms that are submitted using the POST method.

Vulnerability classifications

- CWE-200: Information Exposure
- CWE-384: Session Fixation
- CWE-598: Information Exposure Through Query Strings in GET Request
- CAPEC-593: Session Hijacking

Request

```
OPTIONS /media/soundcloud:tracks:1610873220/70e892cc-fe64-41f4-b0c6-d4ed9fb9a287/stream/hls?secret_token=s-
NVt86r3593y&client_id=KKzJxmw11tYpCs6T24P4uUYhqmjalG6M&track_authorization=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1
NiJ9.eyJnZW8iOiJDQSIsInN1YiI6IiIsInJpZCI6IiIsImlhdCI6MTczMjg1Njk3M30.rOb9sVq2g-xoRptLAjZvMUZNPNfLQ5b-
rD7Vpgk9FNw&stage= HTTP/1.1
Host: api-mobi.soundcloud.com
Accept: */*
Access-Control-Request-Method: GET
Access-Control-Request-Headers: x-datadome-clientid
Origin: https://m.soundcloud.com
Sec-Fetch-Mode: cors
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: same-site
Sec-Fetch-Dest: empty
Referer: https://m.soundcloud.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-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

Response

```
HTTP/1.1 200 OK
Content-Length: 0
Connection: keep-alive
Date: Fri, 29 Nov 2024 05:09:59 GMT
x-robots-tag: noindex
Cache-Control: public, max-age=3600
referrer-policy: no-referrer
x-frame-options: DENY
access-control-max-age: 1728000
x-content-type-options: nosniff
access-control-allow-origin: https://m.soundcloud.com
access-control-allow-headers: Authorization, Content-Type, Device-Locale, X-CSRF-Token, X-Checkout-Token, X-Client-Id, X-
Datadome-ClientId, X-Payments-Id, X-Payments-Token, X-Request-Id
access-control-allow-methods: DELETE, GET, PATCH, POST, PUT
access-control-expose-headers: Date, X-DD-B, X-Set-Cookie
access-control-allow-credentials: true
strict-transport-security: max-age=63072000
Server: am/2
Vary: Origin
X-Cache: Miss from cloudfront
Via: 1.1 9a6f07a84b60a85466bb31603767843c.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: SUNX4XdnCrhbgIeQZOZhQ8OdPXgZdMejyVn2EYTy-vsc7C46oS5bNw==
```

2. Vulnerable JavaScript dependency

Summary

Severity:	**Low**
Confidence:	**Tentative**
Host:	**https://m.sndcdn.com**
Path:	**/_next/static/chunks/main-d39e36461395347a8b66.js**

Issue detail

We observed a vulnerable JavaScript library.

We detected **nextjs** version **10.0.0**, which has the following vulnerabilities:

- CVE-2021-37699: Open Redirect in Next.js
- CVE-2021-39178: XSS in Image Optimization API
- CVE-2021-43803: Unexpected server crash in Next.js versions
- CVE-2022-23646: Improper CSP in Image Optimization API
- CVE-2023-46298: Next.js missing cache-control header may lead to CDN caching empty reply

Issue background

The use of third-party JavaScript libraries can introduce a range of DOM-based vulnerabilities, including some that can be used to hijack user accounts like DOM-XSS.

Common JavaScript libraries typically enjoy the benefit of being heavily audited. This may mean that bugs are quickly identified and patched upstream, resulting in a steady stream of security updates that need to be applied. Although it may be tempting to ignore updates, using a library with missing security patches can make your website exceptionally easy to exploit. Therefore, it's important to ensure that any available security updates are applied promptly.

Some library vulnerabilities expose every application that imports the library, but others only affect applications that use certain library features. Accurately identifying which library vulnerabilities apply to your website can be difficult, so we recommend applying all available security updates regardless.

Issue remediation

Develop a patch-management strategy to ensure that security updates are promptly applied to all third-party libraries in your application. Also, consider reducing your attack surface by removing any libraries that are no longer in use.

Vulnerability classifications

- CWE-1104: Use of Unmaintained Third Party Components
- A9: Using Components with Known Vulnerabilities

Request

```
GET /_next/static/chunks/main-d39e36461395347a8b66.js HTTP/1.1
Host: m.sndcdn.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: */*
X-Requested-With: com.twelve_steps.twelve_steps
```

```
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://m.soundcloud.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: application/javascript; charset=utf-8
Date: Fri, 18 Oct 2024 02:05:08 GMT
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Access-Control-Max-Age: 3000
Last-Modified: Fri, 04 Oct 2024 18:54:24 GMT
Etag: W/"d0ba2227384368134f42833839c18586"
X-Amz-Server-Side-Encryption: AES256
Cache-Control: public, max-age=31536000, immutable
X-Amz-Version-Id: A.ofK7ib4fv0gDH45EgnRolkA5k2d0Py
Server: AmazonS3
Vary: Accept-Encoding
X-Cache: Hit from cloudfront
Via: 1.1 a1ba4b0527e41da66664ba375de24b7c.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C1
X-Amz-Cf-Id: g8yXpL9f4Bcley3pskXTQ-5Mk4zfKPkC24JkX07Y2GXXMVhtsF6g0g==
Age: 3639867

_N_E=(window.webpackJsonp_N_E=window.webpackJsonp_N_E||[]).push([[48],{"7ugj":function(t,e){function r(){return
t.exports=r=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var r=argumen
...[SNIP]...
r("6Omi")),m=p(r("xWJi")),y=r("JbmF"),g=p(r("oJk8")),w=r("BWF2"),E=r("+N4r"),b=r("nJ9T"),_=h(r("nZ9i")),x=h(r("0VSX")),S=r("
zRES"),L=p(r("GZWh")),P=h(r("UUsM")),T=p(r("8e9H")),k=r("VXMs"),N=JSON.parse(document.getElementById("__NEXT_DA
TA__").textContent);window.__NEXT_DATA__=N;e.version="10.0.0";var
A=N.props,O=N.err,j=N.page,C=N.query,R=N.buildId,M=N.assetPrefix,F=N.runtimeConfig,I=N.dynamicIds,B=N.isFallback,D=
N.head,G=N.locales,H=N.locale,q=N.defaultLocale,U=M||"";r.p="".concat(U,"/_next/"
...[SNIP]...
```

3. Strict transport security not enforced

There are 19 instances of this issue:

- https://emmxuq-cdn-settings.appsflyersdk.com/android/v1/b8f2b4cfb63d3a01ab23168079a65fe4e1df1116866bdd83993e9516912b05a4/settings
- https://emmxuq-conversions.appsflyersdk.com/api/v6.13/androidevent
- https://emmxuq-dlsdk.appsflyersdk.com/v1.0/android/com.twelve_steps.twelve_steps
- https://emmxuq-launches.appsflyersdk.com/api/v6.13/androidevent
- https://gmscompliance-pa.googleapis.com/google.internal.gmscore.gmscompliance.v1.GmsCompliance/GetEnforcement
- https://growth-pa.googleapis.com/google.internal.identity.growth.v1.GrowthApiService/GetPromos
- https://i1.sndcdn.com/avatars-Qke9HoPFUSfIuy9C-OX2MVQ-t120x120.jpg
- https://i1.sndcdn.com/avatars-Qke9HoPFUSfIuy9C-OX2MVQ-t240x240.jpg
- https://i1.sndcdn.com/avatars-Qke9HoPFUSfIuy9C-OX2MVQ-t500x500.jpg
- https://inbox.google.com/sync/el2
- https://m.sndcdn.com/_next/static
- https://securepubads.g.doubleclick.net/pagead/managed/js/gpt/m202411180101/pubads_impl.js
- https://securepubads.g.doubleclick.net/pagead/ppub_config

- https://securepubads.g.doubleclick.net/tag/js/gpt.js
- https://securitydomain-pa.googleapis.com/google.internal.identity.securitydomain.v1.SecurityDomainService/GetSecurityDomain
- https://securitydomain-pa.googleapis.com/google.internal.identity.securitydomain.v1.SecurityDomainService/JoinSecurityDomain
- https://style.sndcdn.com/fonts/soundcloud-sans-500-cf1a3e1fb4cee50fe430b572d2c855b4.woff2
- https://style.sndcdn.com/fonts/soundcloud-sans-700-4d19511ea677f5ec5c828f0258549ec4.woff2
- https://style.sndcdn.com/fonts/soundcloud-sans-900-03bbceefe9659e9d9cee10e885a88dc2.woff2

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

3.1. https://emmxuq-cdn-settings.appsflyersdk.com/android/v1/b8f2b4cfb63d3a01ab23168079a65fe4e1df1116866bdd83993e9516912b05a4/settings

Summary

Severity:	**Low**
Confidence:	**Certain**

Host: **https://emmxuq-cdn-settings.appsflyersdk.com**

Path: **/android/v1/b8f2b4cfb63d3a01ab23168079a65fe4e1df1116866bdd83993e9516912b05a4/settings**

Request

```
GET /android/v1/b8f2b4cfb63d3a01ab23168079a65fe4e1df1116866bdd83993e9516912b05a4/settings HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; sdk_gphone_x86 Build/RSR1.201013.001)
Host: emmxuq-cdn-settings.appsflyersdk.com
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 200 OK
Content-Type: application/json
Content-Length: 45
Server: awselb/2.0
Date: Thu, 19 Sep 2024 09:51:46 GMT
X-Amz-Meta-Af-Auth-V1: d509a205680c
Via: 1.1 ac1cb1fdb7cf3984f94f9f190169eb3a.cloudfront.net (CloudFront)
Age: 6117231
X-Af-Date: 1732856738
X-Cache: Hit from cloudfront
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: 5QlZxlvoFJo7vVmaSgfuro5xxH0vC2y32SvWtXus1j8irdHK0SmMOg==

{"features":{},"ver":"default.v1.1637149529"}
```

3.2. https://emmxuq-conversions.appsflyersdk.com/api/v6.13/androidevent

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://emmxuq-conversions.appsflyersdk.com**

Path: **/api/v6.13/androidevent**

Request

```
POST /api/v6.13/androidevent?app_id=com.twelve_steps.twelve_steps&buildnumber=6.13.0 HTTP/1.1
Content-Type: application/octet-stream
Content-Length: 3304
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; sdk_gphone_x86 Build/RSR1.201013.001)
Host: emmxuq-conversions.appsflyersdk.com
Connection: keep-alive
Accept-Encoding: gzip, deflate, br

..T2l..&m.g...k.5m..nWY.Y.z,.;)2.....mY.m....hK.Z_...M.9Q8z."c..X...4.....j....."...1
   .n!..l#].....&t..R..X.7.a.....a....To.......s2F.9..W...o....E.8...O-.E...l...'.+....n.p~%u..aS.P.X....4..?YW.7.
...[SNIP]...
```

Response

```
HTTP/2 403 Forbidden
Content-Length: 9
Date: Fri, 29 Nov 2024 05:05:45 GMT
X-Cache: Error from cloudfront
Via: 1.1 1a0361f1d6eeb33d623d41bfabfa3e8e.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C1
X-Amz-Cf-Id: ckZh1SeVFDRik3lmAmZ92bNg6T6wKYOOlHTaqA64rAmjzLfZ5qqklg==

forbidden
```

3.3. https://emmxuq-dlsdk.appsflyersdk.com/v1.0/android/com.twelve_steps.twelve_steps

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://emmxuq-dlsdk.appsflyersdk.com**
Path:	**/v1.0/android/com.twelve_steps.twelve_steps**

Request

```
POST /v1.0/android/com.twelve_steps.twelve_steps?
af_sig=c75a71df74d88abaa516b61cc7493a74dd9855a1635936361e0962c84c2b0533&sdk_version=6.13 HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; sdk_gphone_x86 Build/RSR1.201013.001)
Host: emmxuq-dlsdk.appsflyersdk.com
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
Content-Length: 246

{"os":"11","gaid":{"type":"unhashed","value":"f20fbe71-dba0-4c12-8b2e-6cbbc3d4cdfe"},"is_first":false,"lang":"en-
US","type":"sdk_gphone_x86","request_id":"1732856734123-8428588531524320033","timestamp
...[SNIP]...
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Content-Length: 32
Date: Fri, 29 Nov 2024 05:05:37 GMT
Server: http-kit
X-Cache: Miss from cloudfront
Via: 1.1 18b0fca4845f3542d7f0566683e26626.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: F3IYEvVglweSKyYckNj3FoxqIS-SOA7OM8i2A1Ftm2baUrQ_bwZubg==

{"found":false,"click_event":{}}
```

3.4. https://emmxuq-launches.appsflyersdk.com/api/v6.13/androidevent

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://emmxuq-launches.appsflyersdk.com**
Path:	**/api/v6.13/androidevent**

Request

```
POST /api/v6.13/androidevent?app_id=com.twelve_steps.twelve_steps&buildnumber=6.13.0 HTTP/1.1
Content-Type: application/octet-stream
Content-Length: 3064
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; sdk_gphone_x86 Build/RSR1.201013.001)
Host: emmxuq-launches.appsflyersdk.com
Connection: keep-alive
Accept-Encoding: gzip, deflate, br

O...;V......O..+.N.(./~....?....r|.....b..WU........;Ib..&......|..0%..r......O.......C.....RBP........
[}.....t/.qD.kY.o+Z&....AI...e......]w{..5.h8.........06.&2$.......{..(......u...........K  .n...L
...[SNIP]...
```

Response

```
HTTP/2 403 Forbidden
Content-Length: 9
Date: Fri, 29 Nov 2024 05:09:29 GMT
X-Cache: Error from cloudfront
Via: 1.1 ede5c8e7b29cc9290d2f384042d78428.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YTO50-P3
X-Amz-Cf-Id: d5HP1bF9Igg2GvsBPgAiWWO-qo9cozPwi0TxmYiuX4ashHYj6b-QNQ==

forbidden
```

3.5. 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: 59494090u
Content-Length: 8253

... 8

.........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 05:05:27 GMT
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Grpc-Status: 0
Endpoint-Load-Metrics-Bin: MURd1dnKUTJASQ5iDO0oStQ/
Grpc-Server-Stats-Bin: AAD1JSoCAAAAAA
Pc-High-Bwd-Bin: S2dJWUNn

....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]...
```

3.6. https://growth-pa.googleapis.com/google.internal.identity.growth.v1.GrowthApiService/GetPromos

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://growth-pa.googleapis.com**
Path:	**/google.internal.identity.growth.v1.GrowthApiService/GetPromos**

Request

```
POST /google.internal.identity.growth.v1.GrowthApiService/GetPromos HTTP/1.1
Host: growth-pa.googleapis.com:443
User-Agent: grpc-java-okhttp/1.31.0-SNAPSHOT
Content-Type: application/grpc
Te: trailers
X-Goog-Api-Key: AIzaSyBXuZXPItcw7joqQCtuR9_yQhXffU_khD4
X-Android-Cert: 38918A453D07199354F8B19AF05EC6562CED5788
X-Android-Package: com.google.android.apps.docs
Grpc-Accept-Encoding: gzip
Authorization: Bearer ya29.m.CoYCAQ1IaZgYeMlbcBW-Dov-DtKaSlh7-
hJqct3LMzL_T9VFZXyng9JyBC2crUHEL3ETPwy1XnRus6YTwcIqzQbkK8HDwxHeg9cg2AF6e3TIOHD3MwVRsjuxINACp3KH
QXYgpxy8fYaOVTBA3tz0a00RILhGZQGgT2tjj5Xmq9fuUdx7LxHLF08DgbY9HbWMtP_yQFk4Y9jBof0loKbdNKCbeoNxawVNa
qd9kPQKZybWHO2NibfsiVd2NLCNARz1ICXADhVL-
Eb08uYNsE1zT3lSLbWJyGNyrJgZQqmrqZRke5IvVxjY6gGajMqdQoCe8eo6fgooQaKI-
1y2Xf02VUtMtlWNSsjkPRIJCAESAxDMHBgAGiBEKikild-WL0U22BAec1xh9smiNFIBa7WoIn-
cfze0vCICCAEqK2FDZ1ILQVJrU0FSSVNGUUhHWDJNaUZXWkUyWDR0TVZjdWY0REVEVTdVR2c
Grpc-Timeout: 17391800u
Content-Length: 136
Connection: keep-alive

.....
  .C.........9.    202220370".com.google.android.apps.docs*.2.20.222.03.70.8..en-US..".30:)
.google..RSR1.201013.001..sdk_gphone_x86".
```

Response

```
HTTP/2 200 OK
Content-Disposition: attachment
Content-Type: application/grpc
Date: Fri, 29 Nov 2024 05:05:27 GMT
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Grpc-Status: 0
Content-Disposition: attachment

.....
```

3.7. https://i1.sndcdn.com/avatars-Qke9HoPFUSfluy9C-OX2MVQ-t120x120.jpg

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://i1.sndcdn.com**
Path:	**/avatars-Qke9HoPFUSfluy9C-OX2MVQ-t120x120.jpg**

Request

```
GET /avatars-Qke9HoPFUSfluy9C-OX2MVQ-t120x120.jpg HTTP/2
Host: i1.sndcdn.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.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
```

```
Sec-Fetch-Dest: image
Referer: https://m.soundcloud.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
Content-Type: image/jpeg
Content-Length: 3565
Access-Control-Allow-Headers: Accept, Accept-Encoding, Authorization, Content-Type, Origin
Access-Control-Allow-Methods: GET
Access-Control-Allow-Origin: *
Cache-Control: public,max-age=2341581
Date: Wed, 27 Nov 2024 13:30:38 GMT
X-Cache: Hit from cloudfront
Via: 1.1 8628ab00b77c57209ad876418b745f6e.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: b2JUQfMYl_ljUreBhJ3ZqU0IAn4JlVLEyDCYoeXTw_HFCi3oBOgpJg==
Age: 142743

......JFIF............C......................    ....
   ..



.......

.......................C.............
.......................................................x.x.."..............................
...[SNIP]...
```

3.8. https://i1.sndcdn.com/avatars-Qke9HoPFUSfluy9C-OX2MVQ-t240x240.jpg

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://i1.sndcdn.com**
Path:	**/avatars-Qke9HoPFUSfluy9C-OX2MVQ-t240x240.jpg**

Request

```
GET /avatars-Qke9HoPFUSfluy9C-OX2MVQ-t240x240.jpg HTTP/1.1
Host: i1.sndcdn.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.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://m.soundcloud.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

```
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: image/jpeg
Content-Length: 8758
Access-Control-Allow-Headers: Accept, Accept-Encoding, Authorization, Content-Type, Origin
Access-Control-Allow-Methods: GET
Access-Control-Allow-Origin: *
Cache-Control: public,max-age=2074940
Date: Wed, 27 Nov 2024 13:30:31 GMT
X-Cache: Hit from cloudfront
Via: 1.1 8628ab00b77c57209ad876418b745f6e.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: hdoBmmeyKLzJA2z8-7v7XhLasv4EozGCvcHIGelLL9MdfhOTWxfIpw==
Age: 142744

......JFIF............C.....................    ....
   ..



.......

.......................C.............
............................................................"..............................
...[SNIP]...
```

3.9. https://i1.sndcdn.com/avatars-Qke9HoPFUSfIuy9C-OX2MVQ-t500x500.jpg

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://i1.sndcdn.com**
Path:	**/avatars-Qke9HoPFUSfIuy9C-OX2MVQ-t500x500.jpg**

Request

```
GET /avatars-Qke9HoPFUSfIuy9C-OX2MVQ-t500x500.jpg HTTP/1.1
Host: i1.sndcdn.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.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://m.soundcloud.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: image/jpeg
Content-Length: 25578
Access-Control-Allow-Headers: Accept, Accept-Encoding, Authorization, Content-Type, Origin
Access-Control-Allow-Methods: GET
Access-Control-Allow-Origin: *
Cache-Control: public,max-age=1831475
Date: Thu, 28 Nov 2024 17:53:31 GMT
X-Cache: Hit from cloudfront
Via: 1.1 8628ab00b77c57209ad876418b745f6e.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: YmhHPviZ3uYIBM28zV0ey4Yabwjbcq8mvWeizivq3iD76rzwksHqtA==
Age: 40564

......JFIF............C.....................    ....
   ..



.......

.......................C.............
..........................................................".............................
...[SNIP]...
```

3.10. https://inbox.google.com/sync/el2

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://inbox.google.com**
Path:	**/sync/el2**

Request

```
POST /sync/el2?hl=en_US&c=0 HTTP/2
Host: inbox.google.com
X-Google-Btd: 1
X-Gmail-Btai:
GswBMABQAWgBeAGAAQGIAQGQAQCYAQGwAQC4AQHAAQHIAQHQAQHYAQDgAQHoAQHwAQH4AQCAAgCIAgCQAg
GYAgCgAgCqAgJlbrICSkFuZHJvaWQtR21haWwvNjIxOTY3NzIgKHN3NDExZHA7IDQyMGRwaSkgKGdlbmVyaWNfeDg2X2F
ybSBSU1IxLjIwMTAxMy4wMDEpwAIAyAIZ0AIA2AIA4AIA6AIA8AIA+AIBgAMBiAMBkAMAmAMAoAMAqAMBsAMAuAMAwAM
AyAMA0AMAOBtCHDIwMjAuMDUuMTcuMzEyNjc5MTIxLnJlbGVhc2VIAIACWhVHb29nbGUgc2RrX2dwaG9uZV94ODZggK+1
9///////AWoQQW1lcmljYS9OZXdfWW9ya3ABgAGkmNQdigEAkgEWZWFfSlEyNjZUQzJPUkhITVRHR21pQ5gBxeLSsrcy
User-Agent: Android-Gmail/62196772 (sw411dp; 420dpi) (generic_x86_arm RSR1.201013.001)
Authorization: OAuth
ya29.a0AeDClZDjxSKYIpaYmaJyL0A8u6Rk1H_iWNx3XmKAIfFKXzndBSFaIUJrflCX5aYuRXYxjeBiPMV8Kb1BdTXWIn9mEYk
ByoWZw4rjrk76InRgqSK-JMSN9Gx9WaXeCy1S6K4q-
0NcsYGmPUiwTdvHimhIUZH4dMgulhjQEwJQqEhDfTh8J2VzFJ05IftOUgBIYtgroSSOPJzzsw7wpULNYagiOiBISIZo-
rrbKL2viiqwyxFMVobO_H4ByfpCSwmQ43fypZf5JiwhWnH1n6WEt7NZSv_3TVfnMr9AzpFy0Tz7KBXXCmhVkI8AeWWXvIrzV1
wbDTi7zOAf_IRu-GJ1YMgxVEv2aCgYKAWsSARISFQHGX2MiqzslycKAiTnTx474LvBsrg0355
Content-Type: application/x-protobuf
Accept-Encoding: gzip, deflate, br
Content-Length: 77
```

```
K
....
../.......
9..B5    ..'    e7yB..P.Ke7yB..../!.......?(.8./..../!.......?(.
```

Response

```
HTTP/2 200 OK
Content-Type: application/vnd.google.octet-stream-compressible
Vary: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site
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 05:11:22 GMT
Content-Disposition: attachment; filename="response.bin"; filename*=UTF-8''response.bin
X-Content-Type-Options: nosniff
P3p: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Cross-Origin-Opener-Policy: same-origin-allow-popups
X-Goog-Server-Latency: 28
Gfe-Rtt-Ms: 151
Server: ESF
Content-Length: 0
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
Set-Cookie: NID=519=NB8YrHSbvrKWZwigCjAB3yLIApkLZeeBKXMBUbct9-QI722_QTnujD-aRT_1d-
1Gk0WjGNLhQPnr2mggCRXmAX2Lmyc5cxhp8BRxqWpwddXHSf1b1jp08tweHHEuMesh1ul7LDGLYf82WYHFMIQMABWA2o
XVkRYSvUfPV6no3UfDDLXP0g; expires=Sat, 31-May-2025 05:11:22 GMT; path=/; domain=.google.com; HttpOnly
Set-Cookie: COMPASS=bigtop-
sync=CsMBAAIriVc4UX9z0cAzW1FV_kTIjjHKDBYww6QwK1BbFGoDPn1cA4W1_atRww7avYD77iwqHfssRkTd3qMNYn2nz3
1b5FmUX8mtCSNWDZuIogdCwcJhUdTstub4huvkkqXdamHk9Qo587TmbgLAsVriWzQdamY9REAuy3mLC1K465M-
yPBN7aR1_oJTQzpjyFRTIX850rRARWctV_HiWbh6Tz4VJHw7nqIp1JVg8nGtrdDS_HnnH4hptHAjze1CvD49DyIGELS6qroGG
uoBAAIriVdBttfLFoiCZoTZ1zEiZ4nebYMjvltBpLKTF403lHEdt1auE0Xbfc7hMJf_5f508MVTN7dvnJnxQHGaXLhEB_mzPADs-
IDQ4Aw8oti60DUlIqKqgWwnvkco9dsQhBu8i9OHfroe9lbOD8v6nlgK8zsqt8H8M5K0Z-7JmW-
quxGF1XidTRh14TcFR0nx_bO8htQWfJ_Lgb5a7eDT6DzmMGEYObCnimihnQP7YfPfUDALV6xXmpPvCu4KhVBJgpkaqeZo0E
PddZqiN7DkmgLIIH9LNpID-SsGEGK-HOeczLO69tJ5JMCvMAE; expires=Mon, 09-Dec-2024 05:11:22 GMT; path=/sync;
Secure; HttpOnly
Alt-Svc: clear
```

3.11. https://m.sndcdn.com/_next/static

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://m.sndcdn.com**
Path:	**/_next/static**

Issue detail

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

Request

```
GET /_next/static/css/32ac4681726a69bdbbb0.css HTTP/1.1
Host: m.sndcdn.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.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: style
Referer: https://m.soundcloud.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: text/css; charset=utf-8
Date: Wed, 18 Sep 2024 20:51:36 GMT
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Access-Control-Max-Age: 3000
Last-Modified: Wed, 18 Sep 2024 20:40:44 GMT
Etag: W/"f9c1aae90bd571740b2f4af7e81db67f"
X-Amz-Server-Side-Encryption: AES256
Cache-Control: public, max-age=31536000, immutable
X-Amz-Version-Id: bL2kkCfEOm7PPVg4ouj6JstY4LU5EFAQ
Server: AmazonS3
Vary: Accept-Encoding
X-Cache: Hit from cloudfront
Via: 1.1 a1ba4b0527e41da66664ba375de24b7c.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C1
X-Amz-Cf-Id: hTyRF9u5v7Kde2zAtpGN9pXf-GqPN9g69GV5eVdjU59eXz5qTbjbXA==
Age: 6164278

.ArtworkPlaceholder_Container__3HU6J{display:flex;align-items:center;justify-content:center;background-color:#f3f3f3;background-color:var(--highlight-color);border-radius:3%;width:100%;height:100%}.Ar
...[SNIP]...
```

3.12. https://securepubads.g.doubleclick.net/pagead/managed/js/gpt/m202411180101/pubads_impl.js

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://securepubads.g.doubleclick.net**
Path:	**/pagead/managed/js/gpt/m202411180101/pubads_impl.js**

Request

```
GET /pagead/managed/js/gpt/m202411180101/pubads_impl.js HTTP/2
Host: securepubads.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
Accept: */*
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://m.soundcloud.com/
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
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Server: cafe
Content-Length: 503686
X-Xss-Protection: 0
Date: Thu, 28 Nov 2024 05:32:56 GMT
Expires: Fri, 28 Nov 2025 05:32:56 GMT
Cache-Control: public, immutable, max-age=31536000
Age: 85000
Etag: 14219397196450604588
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 Google LLC
SPDX-License-Identifier: Apache-2.0
*/
/*


Copyright (c) 2015
...[SNIP]...
```

3.13. https://securepubads.g.doubleclick.net/pagead/ppub_config

Summary

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

Path:	**/pagead/ppub_config**

Request

```
GET /pagead/ppub_config?ippd=m.soundcloud.com HTTP/2
Host: securepubads.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
Accept: */*
Origin: https://m.soundcloud.com
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://m.soundcloud.com/
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
Access-Control-Allow-Origin: *
Date: Fri, 29 Nov 2024 05:09:59 GMT
Expires: Fri, 29 Nov 2024 05:09:59 GMT
Cache-Control: private, max-age=3600, stale-while-revalidate=3600
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Server: cafe
Content-Length: 2466
X-Xss-Protection: 0
Set-Cookie: test_cookie=CheckForPermission; expires=Fri, 29-Nov-2024 05:24:59 GMT; path=/; domain=.doubleclick.net; Secure; SameSite=none
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

[["soundcloud.com",null,"m.soundcloud.com",null,null,["115535218"]],[],[],null,null,[["115535218",
[["liveintent.indexexchange.com",null,1],["openx.net",null,1],["uidapi.com",null,1],["id5-sync.com",nu
...[SNIP]...
```

3.14. https://securepubads.g.doubleclick.net/tag/js/gpt.js

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://securepubads.g.doubleclick.net**
Path:	**/tag/js/gpt.js**

Request

```
GET /tag/js/gpt.js HTTP/1.1
Host: securepubads.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
Accept: */*
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

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 05:09:35 GMT
Expires: Fri, 29 Nov 2024 05:09:35 GMT
Cache-Control: private, max-age=900, stale-while-revalidate=3600
Content-Type: text/javascript; charset=UTF-8
Etag: 779 / 20056 / m202411180101 / config-hash: 2173145291705866055
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Server: cafe
Content-Length: 109511
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

(function(sttc){var window=this;if(window.googletag&&googletag.evalScripts)
{googletag.evalScripts();}if(window.googletag&&googletag._loaded_)return;var n,aa=function(a){var b=0;return function(){retur
...[SNIP]...
```

3.15. https://securitydomain-pa.googleapis.com/google.internal.identity.securitydomain.v1.SecurityDomainService/GetSecurityDomain

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://securitydomain-pa.googleapis.com**
Path:	**/google.internal.identity.securitydomain.v1.SecurityDomainService/GetSecurityDomain**

Request

```
POST /google.internal.identity.securitydomain.v1.SecurityDomainService/GetSecurityDomain HTTP/2
Host: securitydomain-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-Api-Key: AIzaSyAP-gfH3qvi6vgHZbSYwQ_XHqV_mXHhzIk
X-Android-Package: com.google.android.gms
X-Android-Cert: 38918A453D07199354F8B19AF05EC6562CED5788
X-Goog-Spatula:
CjYKFmNvbS5nb29nbGUuYW5kcm9pZC5nbXMaHE9KR0tSVDBIR1pOVStMR2E4RjdHVml6dFY0Zz0Y8M6FupvDrb04
Authorization: Bearer
ya29.a0AeDClZB1_7AtuMmWmade3eLCXhf5cl8twjaIG9o8Fa3EK1R6Tis8uWGCCLtherUYaUJokod4HOkbQMsj60sDaDPTv4I
eAgJlaNnrh9yAO0dD178FUp-sc1LQF25Wnt-
zYZNjJZgUgo4oOHz5dEOnDN4jirhA3Wi0ioTC8N9AcYibp2FmE0dTV3kDIhqiEs4iZouoJTgTTuQjm0wuXsMz-
5pVyk6AjEKUpX78NzZLbjWnAqDHG2h90MC3h63tOohjS0AZdRynf7Ri7hB1bjkyXy26_52a5zx9gS6NmvYWDRaNTpEGaGbya
5gFbvNo1VALaP0aCgYKAY8SARISFQHGX2MiR3LgS5F5Mb2AHDK0VSPXZg0330
X-Auth-Time: 1732856880521
Grpc-Accept-Encoding: gzip
Grpc-Timeout: 34904925u
Content-Length: 82

....M
#users/me/securitydomains/chromesync...$0f8cca4c-44b3-4c1d-9d1b-31b2e13fe8e3
```

Response

```
HTTP/2 200 OK
Content-Type: application/grpc
Grpc-Accept-Encoding: identity, deflate, gzip
Content-Disposition: attachment
Date: Fri, 29 Nov 2024 05:08:30 GMT
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Grpc-Status: 0
Endpoint-Load-Metrics-Bin: MfEiI2Ey03NAOWKU9yH//yRASU/gzxI7j9Q/
Grpc-Server-Stats-Bin: AADQ3WkCAAAAAA
Pc-High-Bwd-Bin: S2dJWUFn

....5
#users/me/securitydomains/chromesync..."...........V
```

3.16. https://securitydomain-pa.googleapis.com/google.internal.identity.securitydomain.v1.SecurityDomainService/JoinSecurityDomain

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://securitydomain-pa.googleapis.com**
Path:	**/google.internal.identity.securitydomain.v1.SecurityDomainService/JoinSecurityDomain**

Request

```
POST /google.internal.identity.securitydomain.v1.SecurityDomainService/JoinSecurityDomain HTTP/2
Host: securitydomain-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-Api-Key: AIzaSyAP-gfH3qvi6vgHZbSYwQ_XHqV_mXHhzIk
X-Android-Package: com.google.android.gms
X-Android-Cert: 38918A453D07199354F8B19AF05EC6562CED5788
X-Goog-Spatula:
CjYKFmNvbS5nb29nbGUuYW5kcm9pZC5nbXMaHE9KR0tSVDBIR1pOVStMR2E4RjdHVml6dFY0Zz0Y8M6FupvDrb04
Authorization: Bearer
ya29.a0AeDClZB1_7AtuMmWmade3eLCXhf5cl8twjaIG9o8Fa3EK1R6Tis8uWGCCLtherUYaUJokod4HOkbQMsj60sDaDPTv4l
eAgJlaNnrh9yAO0dD178FUp-sc1LQF25Wnt-
zYZNjJZgUgo4oOHz5dEOnDN4jirhA3Wi0ioTC8N9AcYibp2FmE0dTV3kDIhqiEs4iZouoJTgTTuQjm0wuXsMz-
5pVyk6AjEKUpX78NzZLbjWnAqDHG2h90MC3h63tOohjS0AZdRynf7Ri7hB1bjkyXy26_52a5zx9gS6NmvYWDRaNTpEGaGbya
5gFbvNo1VALaP0aCgYKAY8SARISFQHGX2MiR3LgS5F5Mb2AHDK0VSPXZg0330
X-Auth-Time: 1732856862604
Grpc-Accept-Encoding: gzip
Grpc-Timeout: 34934338u
Content-Length: 416

.....
%
#users/me/securitydomains/chromesync...
husers/me/members/BCtqB8vJCdCu5XL1FEDQXL2_alU0av4MjVFDrz7tXPDe8mujd0xZ-
OSc7Ui0PF2KKOGIOq_lK7iL2PhiQ3ZQ5oE.A.+j...    ...r..@.\..jU4j...QC.>.\...k.wLY....H.
...[SNIP]...
```

Response

```
HTTP/2 200 OK
Content-Type: application/grpc
Grpc-Accept-Encoding: identity, deflate, gzip
Content-Length: 0
Date: Fri, 29 Nov 2024 05:08:00 GMT
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Grpc-Status: 6
Grpc-Message: Requested entity already exists
Endpoint-Load-Metrics-Bin: MSRHOuHHnHNAOeVuvVTHzCVASWFnfvkVN9E/
Grpc-Server-Stats-Bin: AABxLJMFAAAAAA
Pc-High-Bwd-Bin: S2dJWUJR
Google.internal.identity.securitydomain.v1.joinsecuritydomainerrordetail-Bin:
CjcKNQojdXNlcnMvbWUvc2VjdXJpdHlkb21haW5zL2Nocm9tZXN5bmMQhwEiCwjc+P65BhCI+bBW
Grpc-Status-Details-Bin:
CAYSH1JlcXVlc3RlZCBlbnRpdHkgYWxyZWFkeSBleGlzdHMamQEKXHR5cGUuZ29vZ2xlYXBpcy5jb20vZ29vZ2xlLmludGVyb
mFsLmlkZW50aXR5LnNlY3VyaXR5ZG9tYWluLnYxLkpvaW5TZWN1cml0eURvbWFpbkVycm9yRGV0YWlsEjkKNwo1CiN1c2V
ycy9tZS9zZWN1cml0eWRvbWFpbnMvY2hyb21lc3luYxCHASILCNz4/rkGEIj5sFY
```

3.17. https://style.sndcdn.com/fonts/soundcloud-sans-500-cf1a3e1fb4cee50fe430b572d2c855b4.woff2

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://style.sndcdn.com**

Path: **/fonts/soundcloud-sans-500-cf1a3e1fb4cee50fe430b572d2c855b4.woff2**

Request

```
GET /fonts/soundcloud-sans-500-cf1a3e1fb4cee50fe430b572d2c855b4.woff2 HTTP/1.1
Host: style.sndcdn.com
Origin: https://m.soundcloud.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: */*
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: font
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: font/woff2
Content-Length: 22996
Date: Wed, 18 Sep 2024 17:37:42 GMT
Access-Control-Allow-Origin: https://m.soundcloud.com
Access-Control-Allow-Methods: GET
Access-Control-Max-Age: 3600
Access-Control-Allow-Credentials: true
Last-Modified: Thu, 12 Sep 2024 20:10:05 GMT
Etag: "97c0e7a42bac111dce1dcaa2ebbdb2f3"
X-Amz-Server-Side-Encryption: AES256
Cache-Control: public, max-age=31536000
Accept-Ranges: bytes
Server: AmazonS3
Vary: Origin,Access-Control-Request-Headers,Access-Control-Request-Method
X-Cache: Hit from cloudfront
Via: 1.1 b7321b4add4495066f8401239ad07f94.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: dc9AVH7hLSepJorR3lfb-QkiLnfb5aqCYl6CNpY8xZNolRLccxnC5g==
Age: 6175912

wOF2......Y.......&...Yu...A........................V..D.`..V..
..P..J.6.$..H..f.. ..R..].....5x..*.........[3..Vr.I.^dP.8. .....?%........?d...#G....<.
D\k..cT-....H.O...n.DN._r...SQ.c..*xc..}c.f.E
...[SNIP]...
```

3.18. https://style.sndcdn.com/fonts/soundcloud-sans-700-4d19511ea677f5ec5c828f0258549ec4.woff2

Summary

Severity: **Low**

Confidence: **Certain**

Host: **https://style.sndcdn.com**

Path:	**/fonts/soundcloud-sans-700-4d19511ea677f5ec5c828f0258549ec4.woff2**

Request

```
GET /fonts/soundcloud-sans-700-4d19511ea677f5ec5c828f0258549ec4.woff2 HTTP/2
Host: style.sndcdn.com
Origin: https://m.soundcloud.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: */*
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: font
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
Content-Type: font/woff2
Content-Length: 23056
Date: Tue, 10 Sep 2024 13:22:36 GMT
Access-Control-Allow-Origin: https://m.soundcloud.com
Access-Control-Allow-Methods: GET
Access-Control-Max-Age: 3600
Access-Control-Allow-Credentials: true
Last-Modified: Mon, 09 Sep 2024 13:29:33 GMT
Etag: "3ed18f6245d38bc2e19f37e2327d08a5"
X-Amz-Server-Side-Encryption: AES256
Cache-Control: public, max-age=31536000
Accept-Ranges: bytes
Server: AmazonS3
Vary: Origin,Access-Control-Request-Headers,Access-Control-Request-Method
X-Cache: Hit from cloudfront
Via: 1.1 b7321b4add4495066f8401239ad07f94.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: wsuMAj1Uk-eCikoBNaOZ4xh7t5I5DifyjOqYIuIXmDTRuNzcc2OPfA==
Age: 6882419

wOF2......Z.......&...Y....A........................V..D.`..V..
.....}.6.$..H..f.. ..R..]...z...6.... 4.....r.8.'..?
i(iU......1.......0...mV....#3.......W...h!.t..9..7..]..T.S~........-........T...
...[SNIP]...
```

3.19. https://style.sndcdn.com/fonts/soundcloud-sans-900-03bbceefe9659e9d9cee10e885a88dc2.woff2

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://style.sndcdn.com**

Path: **/fonts/soundcloud-sans-900-03bbceefe9659e9d9cee10e885a88dc2.woff2**

Request

```
GET /fonts/soundcloud-sans-900-03bbceefe9659e9d9cee10e885a88dc2.woff2 HTTP/2
Host: style.sndcdn.com
Origin: https://m.soundcloud.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: */*
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: font
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
Content-Type: font/woff2
Content-Length: 21872
Date: Thu, 19 Sep 2024 09:55:24 GMT
Access-Control-Allow-Origin: https://m.soundcloud.com
Access-Control-Allow-Methods: GET
Access-Control-Max-Age: 3600
Access-Control-Allow-Credentials: true
Last-Modified: Thu, 12 Sep 2024 20:10:06 GMT
Etag: "339bdcb44b2d3c42bb69e5e77a583ad8"
X-Amz-Server-Side-Encryption: AES256
Cache-Control: public, max-age=31536000
Accept-Ranges: bytes
Server: AmazonS3
Vary: Origin,Access-Control-Request-Headers,Access-Control-Request-Method
X-Cache: Hit from cloudfront
Via: 1.1 b7321b4add4495066f8401239ad07f94.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: 6d5JctgPbEAGIl0lDTnUa8DYgMfQWOIvjOujEaZoBDZJGlcBYYRnDg==
Age: 6117251

wOF2......Up......&8..U....A........................V..D.`..V..
..H....6.$..H..f.. ..R..]...~.7ps..e.=.m&.....@.;`.........@$~.......5d.av.[....".E.....V..2..j......8.&.{fa+#....\...x....HL..(..../]
...[SNIP]...
```

---

4. Content security policy: allows untrusted script execution

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://m.soundcloud.com**

Path: **/12stepsapp/on-awakening/s-NVt86r3593y**

Issue detail

The content security policy fails to prevent untrusted JavaScript from being executed. As a result, it may fail to mitigate cross-site scripting attacks.

The policy has the following issues:

The policy allows global wildcard URLs which allows arbitrary scripts to be executed.

The policy allows data: URLs which allows arbitrary scripts to be executed.

Issue background

Content Security Policy (CSP) is a security mechanism designed to mitigate cross-site scripting attacks by disabling dangerous behaviours such as untrusted JavaScript execution. Websites can specify their security policy in a response header or meta tag, enabling fine-grained control over dangerous features like scripts and stylesheets.

Issue remediation

Mitigate cross-site scripting by avoiding 'unsafe-inline', 'unsafe-eval', data: URLs, and global wildcards in script directives. Use a secure, random nonce of at least 8 characters 'nonce-RANDOM' to prevent untrusted JavaScript execution.

References

- Web Security Academy: What is CSP?
- Web Security Academy: What is XSS?
- Web Security Academy: Mitigating XSS attacks using CSP
- Web Security Academy: Preventing XSS
- Content Security Policy (CSP)

Vulnerability classifications

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
- CWE-116: Improper Encoding or Escaping of Output
- CWE-159: Failure to Sanitize Special Element
- CAPEC-588: DOM-Based XSS

Request

```
GET /12stepsapp/on-awakening/s-NVt86r3593y?
si=1d284dff98974cb183c9f96d537444f1&utm_source=clipboard&utm_medium=text&utm_campaign=social_sharing HTTP/1.1
Host: m.soundcloud.com
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
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.twelve_steps.twelve_steps
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
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: sc_anonymous_id=585810-837106-950987-811574; path=/; expires=Mon, 27 Nov 2034 05:09:33 GMT; domain=.soundcloud.com
Cache-Control: private, max-age=0, no-cache, no-store
Content-Security-Policy: frame-ancestors 'none';
X-Frame-Options: DENY
Referrer-Policy: never, no-referrer
X-Content-Type-Options: nosniff
Feature-Policy: accelerometer none; ambient-light-sensor none; autoplay none; battery none; camera none; display-capture none; document-domain none; fullscreen none; geolocation none; gyroscope none; magnetometer none; microphone none; midi none; picture-in-picture none; sync-xhr none; usb none; wake-lock none
Etag: "1130d-1zKjkhWHDWpKdwW365h9bK5qCko"
Date: Fri, 29 Nov 2024 05:09:33 GMT
Strict-Transport-Security: max-age=63072000
Server: am/2
Vary: Accept,Accept-Encoding,Accept-Language,Origin
X-Cache: Miss from cloudfront
Via: 1.1 ea419f8269940bd7231c70acd36c430c.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: 47mt75G32Scs3bIIcMxSZt79zPma0WQT_Gu3EHMfx4JnII-ItzUOSA==

<!DOCTYPE html><html lang="en" style="min-width:fit-content"><head><script>
(function () {
window.ddjskey = '7FC6D561817844F25B65CDD97F28A1';
window.ddoptions =
...[SNIP]...
```

5. Content security policy: allows untrusted style execution

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://m.soundcloud.com**
Path:	**/12stepsapp/on-awakening/s-NVt86r3593y**

Issue detail

The content security policy fails to prevent untrusted style execution. As a result, it may fail to mitigate style based data exfiltration.

The policy allows global wildcard URLs which allows arbitrary styles to be executed.

The policy allows data: URLs which allows arbitrary styles to be executed.

Issue background

Content Security Policy (CSP) is a security mechanism designed to mitigate cross-site scripting attacks by disabling dangerous behaviours such as untrusted JavaScript execution. Websites can specify their security policy in a response header or meta tag, enabling fine-grained control over dangerous features like scripts and stylesheets.

Issue remediation

Mitigate style-based data exfiltration by avoiding 'unsafe-inline', data: URLs, and global wildcards in style directives. Use a secure, random nonce of at least 8 characters 'nonce-RANDOM' in the relevant directive.

References

- Web Security Academy: What is CSP?
- PortSwigger Research: Blind CSS exfiltration
- PortSwigger Research: Offensive CSS research
- Content Security Policy (CSP)

Vulnerability classifications

- CWE-116: Improper Encoding or Escaping of Output
- CWE-159: Failure to Sanitize Special Element
- CAPEC-468: Generic Cross-Browser Cross-Domain Theft

Request

```
GET /12stepsapp/on-awakening/s-NVt86r3593y?
si=1d284dff98974cb183c9f96d537444f1&utm_source=clipboard&utm_medium=text&utm_campaign=social_sharing HTTP/1.1
Host: m.soundcloud.com
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
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.twelve_steps.twelve_steps
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
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: sc_anonymous_id=585810-837106-950987-811574; path=/; expires=Mon, 27 Nov 2034 05:09:33 GMT;
domain=.soundcloud.com
Cache-Control: private, max-age=0, no-cache, no-store
Content-Security-Policy: frame-ancestors 'none';
X-Frame-Options: DENY
Referrer-Policy: never, no-referrer
X-Content-Type-Options: nosniff
Feature-Policy: accelerometer none; ambient-light-sensor none; autoplay none; battery none; camera none; display-capture
none; document-domain none; fullscreen none; geolocation none; gyroscope none; magnetometer none; microphone none;
midi none; picture-in-picture none; sync-xhr none; usb none; wake-lock none
Etag: "1130d-1zKjkhWHDWpKdwW365h9bK5qCko"
Date: Fri, 29 Nov 2024 05:09:33 GMT
Strict-Transport-Security: max-age=63072000
Server: am/2
Vary: Accept,Accept-Encoding,Accept-Language,Origin
X-Cache: Miss from cloudfront
Via: 1.1 ea419f8269940bd7231c70acd36c430c.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: 47mt75G32Scs3bIIcMxSZt79zPma0WQT_Gu3EHMfx4JnII-ItzUOSA==

<!DOCTYPE html><html lang="en" style="min-width:fit-content"><head><script>
(function () {
```

```
window.ddjskey = '7FC6D561817844F25B65CDD97F28A1';
window.ddoptions =
...[SNIP]...
```

6. Content security policy: allows form hijacking

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://m.soundcloud.com**
Path:	**/12stepsapp/on-awakening/s-NVt86r3593y**

Issue detail

The content security policy doesn't prevent form hijacking, where attackers with HTML injection hijack forms using action attributes. This can lead to credential theft by autofilling passwords from a manager and sending them to an attacker's server upon form submission.

Issue background

Content Security Policy (CSP) is a security mechanism designed to mitigate cross-site scripting attacks by disabling dangerous behaviours such as untrusted JavaScript execution. Websites can specify their security policy in a response header or meta tag, enabling fine-grained control over dangerous features like scripts and stylesheets.

Issue remediation

We recommend using the form-action directive in the CSP response header to control form post destinations. If no form actions are used, set form-action to 'none' to block untrusted forms. For applications without external form URLs, use 'self' to allow only same-origin URLs. If needed, allow list hosts for external URL form submissions, but be aware this lets attackers submit to these external resources.

References

- PortSwigger Research: Stealing passwords from infosec Mastodon - without bypassing CSP
- Web Security Academy: What is CSP?
- Content Security Policy (CSP)

Vulnerability classifications

- CWE-116: Improper Encoding or Escaping of Output

Request

```
GET /12stepsapp/on-awakening/s-NVt86r3593y?
si=1d284dff98974cb183c9f96d537444f1&utm_source=clipboard&utm_medium=text&utm_campaign=social_sharing HTTP/1.1
Host: m.soundcloud.com
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
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.twelve_steps.twelve_steps
```

```
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
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: sc_anonymous_id=585810-837106-950987-811574; path=/; expires=Mon, 27 Nov 2034 05:09:33 GMT; domain=.soundcloud.com
Cache-Control: private, max-age=0, no-cache, no-store
Content-Security-Policy: frame-ancestors 'none';
X-Frame-Options: DENY
Referrer-Policy: never, no-referrer
X-Content-Type-Options: nosniff
Feature-Policy: accelerometer none; ambient-light-sensor none; autoplay none; battery none; camera none; display-capture none; document-domain none; fullscreen none; geolocation none; gyroscope none; magnetometer none; microphone none; midi none; picture-in-picture none; sync-xhr none; usb none; wake-lock none
Etag: "1130d-1zKjkhWHDWpKdwW365h9bK5qCko"
Date: Fri, 29 Nov 2024 05:09:33 GMT
Strict-Transport-Security: max-age=63072000
Server: am/2
Vary: Accept,Accept-Encoding,Accept-Language,Origin
X-Cache: Miss from cloudfront
Via: 1.1 ea419f8269940bd7231c70acd36c430c.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: 47mt75G32Scs3bIIcMxSZt79zPma0WQT_Gu3EHMfx4JnII-ltzUOSA==

<!DOCTYPE html><html lang="en" style="min-width:fit-content"><head><script>
(function () {
window.ddjskey = '7FC6D561817844F25B65CDD97F28A1';
window.ddoptions =
...[SNIP]...
```

7. TLS cookie without secure flag set

There are 2 instances of this issue:

- https://inbox.google.com/sync/el2
- https://m.soundcloud.com/12stepsapp/on-awakening/s-NVt86r3593y

Issue background

If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site. Even if the domain that issued the cookie does not host any content that is accessed over HTTP, an attacker may be able to use links of the form http://example.com:443/ to perform the same attack.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on 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 secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTPS. If cookies are used to transmit session tokens, then areas of the application that are accessed over HTTPS should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications.

Vulnerability classifications

- CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

---

7.1. https://inbox.google.com/sync/el2

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://inbox.google.com**
Path:	**/sync/el2**

Issue detail

The following cookie was issued by the application and does not have the secure flag set:

- NID

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.

Request

```
POST /sync/el2?hl=en_US&c=0 HTTP/2
Host: inbox.google.com
X-Google-Btd: 1
X-Gmail-Btai:
GswBMABQAWgBeAGAAQGIAQGQAQCYAQGwAQC4AQHAAQHIAQHQAQHYAQDgAQHoAQHwAQH4AQCAAgCIAgCQAg
GYAgCgAgCqAgJlbrICSkFuZHJvaWQtR21haWwvNjIxOTY3NzIgKHN3NDExZHA7IDQyMGRwaSkgKGdlbmVyaWNfeDg2X2F
ybSBSU1IxLjIwMTAxMy4wMDEpwAIAyAIZ0AIA2AIA4AIA6AIA8AIA+AIBgAMBiAMBkAMAmAMAoAMAqAMBsAMAuAMAwAM
AyAMA0AMAOBtCHDIwMjAuMDUuMTcuMzEyNjc5MTIxLnJlbGVhc2VIAIACWhVHb29nbGUgc2RrX2dwaG9uZV94ODZggK+1
9///////AWoQQW1lcmljYS9OZXdfWW9ya3ABgAGkmNQdigEAkgEWZWFfSlEyNjZUQzJPUkhITVRHR21pQ5gBxeLSsrcy
User-Agent: Android-Gmail/62196772 (sw411dp; 420dpi) (generic_x86_arm RSR1.201013.001)
Authorization: OAuth
ya29.a0AeDClZDjxSKYIpaYmaJyL0A8u6Rk1H_iWNx3XmKAIfFKXzndBSFaIUJrflCX5aYuRXYxjeBiPMV8Kb1BdTXWIn9mEYk
ByoWZw4rjrk76InRgqSK-JMSN9Gx9WaXeCy1S6K4q-
0NcsYGmPUiwTdvHimhlUZH4dMgulhjQEwJQqEhDfTh8J2VzFJ05IftOUgBIYtgroSSOPJzzsw7wpULNYagiOiBlSIZo-
rrbKL2viiqwyxFMVobO_H4ByfpCSwmQ43fypZf5JiwhWnH1n6WEt7NZSv_3TVfnMr9AzpFy0Tz7KBXXCmhVkI8AeWWXvIrzV1
wbDTi7zOAf_IRu-GJ1YMgxVEv2aCgYKAWsSARISFQHGX2MiqzslycKAiTnTx474LvBsrg0355
Content-Type: application/x-protobuf
Accept-Encoding: gzip, deflate, br
Content-Length: 77
```

```
K
....
../.......
9..B5    ..'    e7yB..P.Ke7yB..../!.......?(.8./..../!.......?(.
```

Response

```
HTTP/2 200 OK
Content-Type: application/vnd.google.octet-stream-compressible
Vary: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site
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 05:11:22 GMT
Content-Disposition: attachment; filename="response.bin"; filename*=UTF-8''response.bin
X-Content-Type-Options: nosniff
P3p: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Cross-Origin-Opener-Policy: same-origin-allow-popups
X-Goog-Server-Latency: 28
Gfe-Rtt-Ms: 151
Server: ESF
Content-Length: 0
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
Set-Cookie: NID=519=NB8YrHSbvrKWZwigCjAB3yLIApkLZeeBKXMBUbct9-QI722_QTnujD-aRT_1d-
1Gk0WjGNLhQPnr2mggCRXmAX2Lmyc5cxhp8BRxqWpwddXHSf1b1jp08tweHHEuMesh1uI7LDGLYf82WYHFMIQMABWA2o
XVkRYSvUfPV6no3UfDDLXP0g; expires=Sat, 31-May-2025 05:11:22 GMT; path=/; domain=.google.com; HttpOnly
Set-Cookie: COMPASS=bigtop-
sync=CsMBAAIriVc4UX9z0cAzW1FV_kTIjjHKDBYww6QwK1BbFGoDPn1cA4W1_atRww7avYD77iwqHfssRkTd3qMNYn2nz3
1b5FmUX8mtCSNWDZuIogdCwcJhUdTstub4huvkkqXdamHk9Qo587TmbgLAsVriWzQdamY9REAuy3mLC1K465M-
yPBN7aR1_oJTQzpjyFRTlX850rRARWctV_HiWbh6Tz4VJHw7nqIp1JVg8nGtrdDS_HnnH4hptHAjze1CvD49DyIGELS6qroGG
uoBAAIriVdBttfLFoiCZoTZ1zEiZ4nebYMjvltBpLKTF403lHEdt1auE0Xbfc7hMJf_5f508MVTN7dvnJnxQHGaXLhEB_mzPADs-
IDQ4Aw8oti60DUlIqKqgWwnvkco9dsQhBu8i9OHfroe9lbOD8v6nlgK8zsqt8H8M5K0Z-7JmW-
quxGF1XidTRh14TcFR0nx_bO8htQWfJ_Lgb5a7eDT6DzmMGEYObCnimihnQP7YfPfUDALV6xXmpPvCu4KhVBJgpkaqeZo0E
PddZqiN7DkmgLIIH9LNpID-SsGEGK-HOeczLO69tJ5JMCvMAE; expires=Mon, 09-Dec-2024 05:11:22 GMT; path=/sync;
Secure; HttpOnly
Alt-Svc: clear
```

7.2. https://m.soundcloud.com/12stepsapp/on-awakening/s-NVt86r3593y

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://m.soundcloud.com**
Path:	**/12stepsapp/on-awakening/s-NVt86r3593y**

Issue detail

The following cookie was issued by the application and does not have the secure flag set:

- sc_anonymous_id

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.

Request

```
GET /12stepsapp/on-awakening/s-NVt86r3593y?
si=1d284dff98974cb183c9f96d537444f1&utm_source=clipboard&utm_medium=text&utm_campaign=social_sharing HTTP/1.1
Host: m.soundcloud.com
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
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.twelve_steps.twelve_steps
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
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: sc_anonymous_id=585810-837106-950987-811574; path=/; expires=Mon, 27 Nov 2034 05:09:33 GMT;
domain=.soundcloud.com
Cache-Control: private, max-age=0, no-cache, no-store
Content-Security-Policy: frame-ancestors 'none';
X-Frame-Options: DENY
Referrer-Policy: never, no-referrer
X-Content-Type-Options: nosniff
Feature-Policy: accelerometer none; ambient-light-sensor none; autoplay none; battery none; camera none; display-capture
none; document-domain none; fullscreen none; geolocation none; gyroscope none; magnetometer none; microphone none;
midi none; picture-in-picture none; sync-xhr none; usb none; wake-lock none
Etag: "1130d-1zKjkhWHDWpKdwW365h9bK5qCko"
Date: Fri, 29 Nov 2024 05:09:33 GMT
Strict-Transport-Security: max-age=63072000
Server: am/2
Vary: Accept,Accept-Encoding,Accept-Language,Origin
X-Cache: Miss from cloudfront
Via: 1.1 ea419f8269940bd7231c70acd36c430c.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: 47mt75G32Scs3bIIcMxSZt79zPma0WQT_Gu3EHMfx4JnII-ltzUOSA==

<!DOCTYPE html><html lang="en" style="min-width:fit-content"><head><script>
(function () {
window.ddjskey = '7FC6D561817844F25B65CDD97F28A1';
window.ddoptions =
...[SNIP]...
```

8. Cookie scoped to parent domain

There are 4 instances of this issue:

- https://inbox.google.com/sync/el2
- https://m.soundcloud.com/12stepsapp/on-awakening/s-NVt86r3593y
- https://securepubads.g.doubleclick.net/pagead/ppub_config
- https://www.google.com/httpservice/retry/NotificationActionUploadService/NotificationActionUpload

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

8.1. https://inbox.google.com/sync/el2

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://inbox.google.com**
Path:	**/sync/el2**

Issue detail

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

- NID

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.

Request

```
POST /sync/el2?hl=en_US&c=0 HTTP/2
Host: inbox.google.com
X-Google-Btd: 1
X-Gmail-Btai:
GswBMABQAWgBeAGAAQGIAQGQAQCYAQGwAQC4AQHAAQHIAQHQAQHYAQDgAQHoAQHwAQH4AQCAAgCIAgCQAg
GYAgCgAgCqAgJlbrICSkFuZHJvaWQtR21haWwvNjIxOTY3NzIgKHN3NDExZHA7IDQyMGRwaSkgKGdlbmVyaWNfeDg2X2F
ybSBSU1IxLjIwMTAxMy4wMDEpwAIAyAIZ0AIA2AIA4AIA6AIA8AIA+AIBgAMBiAMBkAMAmAMAoAMAqAMBsAMAuAMAwAM
```

```
AyAMA0AMAOBtCHDIwMjAuMDUuMTcuMzEyNjc5MTIxLnJlbGVhc2VIAIACWhVHb29nbGUgc2RrX2dwaG9uZV94ODZggK+1
9///////AWoQQW1lcmljYS9OZXdfWW9ya3ABgAGkmNQdigEAkgEWZWFfSlEyNjZUQzJPUkhITVRHR21pQ5gBxeLSsrcy
User-Agent: Android-Gmail/62196772 (sw411dp; 420dpi) (generic_x86_arm RSR1.201013.001)
Authorization: OAuth
ya29.a0AeDClZDjxSKYIpaYmaJyL0A8u6Rk1H_iWNx3XmKAIfFKXzndBSFaIUJrfICX5aYuRXYxjeBiPMV8Kb1BdTXWIn9mEYk
ByoWZw4rjrk76InRgqSK-JMSN9Gx9WaXeCy1S6K4q-
0NcsYGmPUiwTdvHimhIUZH4dMguIhjQEwJQqEhDfTh8J2VzFJ05IftOUgBIYtgroSSOPJzzsw7wpULNYagiOiBISIZo-
rrbKL2viiqwyxFMVobO_H4ByfpCSwmQ43fypZf5JiwhWnH1n6WEt7NZSv_3TVfnMr9AzpFy0Tz7KBXXCmhVkI8AeWWXvIrzV1
wbDTi7zOAf_IRu-GJ1YMgxVEv2aCgYKAWsSARISFQHGX2MiqzslycKAiTnTx474LvBsrg0355
Content-Type: application/x-protobuf
Accept-Encoding: gzip, deflate, br
Content-Length: 77


K
....
../.......
9..B5    ..'    e7yB..P.Ke7yB..../!.......?(.8./..../!.......?(.
```

Response

```
HTTP/2 200 OK
Content-Type: application/vnd.google.octet-stream-compressible
Vary: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site
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 05:11:22 GMT
Content-Disposition: attachment; filename="response.bin"; filename*=UTF-8''response.bin
X-Content-Type-Options: nosniff
P3p: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Cross-Origin-Opener-Policy: same-origin-allow-popups
X-Goog-Server-Latency: 28
Gfe-Rtt-Ms: 151
Server: ESF
Content-Length: 0
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
Set-Cookie: NID=519=NB8YrHSbvrKWZwigCjAB3yLIApkLZeeBKXMBUbct9-QI722_QTnujD-aRT_1d-
1Gk0WjGNLhQPnr2mggCRXmAX2Lmyc5cxhp8BRxqWpwddXHSf1b1jp08tweHHEuMesh1uI7LDGLYf82WYHFMIQMABWA2o
XVkRYSvUfPV6no3UfDDLXP0g; expires=Sat, 31-May-2025 05:11:22 GMT; path=/; domain=.google.com; HttpOnly
Set-Cookie: COMPASS=bigtop-
sync=CsMBAAIriVc4UX9z0cAzW1FV_kTIjjHKDBYww6QwK1BbFGoDPn1cA4W1_atRww7avYD77iwqHfssRkTd3qMNYn2nz3
1b5FmUX8mtCSNWDZuIogdCwcJhUdTstub4huvkkqXdamHk9Qo587TmbgLAsVriWzQdamY9REAuy3mLC1K465M-
yPBN7aR1_oJTQzpjyFRTIX850rRARWctV_HiWbh6Tz4VJHw7nqIp1JVg8nGtrdDS_HnnH4hptHAjze1CvD49DyIGELS6qroGG
uoBAAIriVdBttfLFoiCZoTZ1zEiZ4nebYMjvltBpLKTF403IHEdt1auE0Xbfc7hMJf_5f508MVTN7dvnJnxQHGaXLhEB_mzPADs-
IDQ4Aw8oti60DUIIqKqgWwnvkco9dsQhBu8i9OHfroe9lbOD8v6nlgK8zsqt8H8M5K0Z-7JmW-
quxGF1XidTRh14TcFR0nx_bO8htQWfJ_Lgb5a7eDT6DzmMGEYObCnimihnQP7YfPfUDALV6xXmpPvCu4KhVBJgpkaqeZo0E
PddZqiN7DkmgLIIH9LNpID-SsGEGK-HOeczLO69tJ5JMCvMAE; expires=Mon, 09-Dec-2024 05:11:22 GMT; path=/sync;
Secure; HttpOnly
Alt-Svc: clear
```

8.2. https://m.soundcloud.com/12stepsapp/on-awakening/s-NVt86r3593y

Summary

Severity: **Information**

Confidence:	**Certain**
Host:	**https://m.soundcloud.com**
Path:	**/12stepsapp/on-awakening/s-NVt86r3593y**

Issue detail

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

- sc_anonymous_id

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.

Request

```
GET /12stepsapp/on-awakening/s-NVt86r3593y?
si=1d284dff98974cb183c9f96d537444f1&utm_source=clipboard&utm_medium=text&utm_campaign=social_sharing HTTP/1.1
Host: m.soundcloud.com
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
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.twelve_steps.twelve_steps
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
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: sc_anonymous_id=585810-837106-950987-811574; path=/; expires=Mon, 27 Nov 2034 05:09:33 GMT;
domain=.soundcloud.com
Cache-Control: private, max-age=0, no-cache, no-store
Content-Security-Policy: frame-ancestors 'none';
X-Frame-Options: DENY
Referrer-Policy: never, no-referrer
X-Content-Type-Options: nosniff
Feature-Policy: accelerometer none; ambient-light-sensor none; autoplay none; battery none; camera none; display-capture
none; document-domain none; fullscreen none; geolocation none; gyroscope none; magnetometer none; microphone none;
midi none; picture-in-picture none; sync-xhr none; usb none; wake-lock none
Etag: "1130d-1zKjkhWHDWpKdwW365h9bK5qCko"
Date: Fri, 29 Nov 2024 05:09:33 GMT
Strict-Transport-Security: max-age=63072000
Server: am/2
Vary: Accept,Accept-Encoding,Accept-Language,Origin
X-Cache: Miss from cloudfront
Via: 1.1 ea419f8269940bd7231c70acd36c430c.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: 47mt75G32Scs3bIIcMxSZt79zPma0WQT_Gu3EHMfx4JnII-ltzUOSA==

<!DOCTYPE html><html lang="en" style="min-width:fit-content"><head><script>
(function () {
window.ddjskey = '7FC6D561817844F25B65CDD97F28A1';
window.ddoptions =
...[SNIP]...
```

8.3. https://securepubads.g.doubleclick.net/pagead/ppub_config

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://securepubads.g.doubleclick.net**
Path:	**/pagead/ppub_config**

Issue detail

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

- test_cookie

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.

Request

```
GET /pagead/ppub_config?ippd=m.soundcloud.com HTTP/2
Host: securepubads.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
Accept: */*
Origin: https://m.soundcloud.com
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://m.soundcloud.com/
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
Access-Control-Allow-Origin: *
Date: Fri, 29 Nov 2024 05:09:59 GMT
Expires: Fri, 29 Nov 2024 05:09:59 GMT
Cache-Control: private, max-age=3600, stale-while-revalidate=3600
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Server: cafe
Content-Length: 2466
X-Xss-Protection: 0
Set-Cookie: test_cookie=CheckForPermission; expires=Fri, 29-Nov-2024 05:24:59 GMT; path=/; domain=.doubleclick.net;
```

```
Secure; SameSite=none
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

[["soundcloud.com",null,"m.soundcloud.com",null,null,["115535218"]],[],[],null,null,[["115535218",
[["liveintent.indexexchange.com",null,1],["openx.net",null,1],["uidapi.com",null,1],["id5-sync.com",nu
...[SNIP]...
```

8.4. https://www.google.com/httpservice/retry/NotificationActionUploadService/NotificationActionUpload

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://www.google.com**
Path:	**/httpservice/retry/NotificationActionUploadService/NotificationActionUpload**

Issue detail

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

- NID

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.

Request

```
GET /httpservice/retry/NotificationActionUploadService/NotificationActionUpload?
reqpId=CnwKBWVuX1VTENOWpboGIhBBbWVyaWNhL05Id19Zb3JrKAEwAToCMTFCDzE1LjQ2LjM2LnZlLng4NkpAMmE3Ym
NhOGNiYTBlNzViNDAxZGQ4Mzc4OWFhOWJjYTRjMzNjMjQ0MmZlYjA1MjJmMzcwNTBiYjZkMTYwZjI4NlgAEqoBChoKEQoE
d3guZhACGZQDAAAAAAAAEgAqAwicAhIbGhMIvurqiuKAigMVh0ZNAx1-6S-
DKNOWpboGGiISIDYzwrAgLyA0McKwIMK3IFNlZSBmdWxsIGZvcmVjYXN0IksKSQizATgBYgJlbnoFCBcQwHB6BQgCEMBw
eggIjgMQgJqeAXoICKYDEICangF6CAinAxCAmp4BgAEBigEECAAQAKIBBAoCVVO4AQEoAg%3D%3D&fmt=bin HTTP/2
Host: www.google.com
User-Agent: Mozilla/5.0 (Linux; Android 11; en-us; 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 GoogleApp/15.46.36.ve.x86
X-Client-Data: apoaH4sIAAAAAAAAAJ2Wa4wb13XHG4VtDFcojMA7CYp-
WvRDvxAYLI_DDwJ677zIGQ7JOySXHH4hZrjk5WP5flySn6woUqXVWpatpJWbxNK-vLXXqWWrlmXZlhTbkV-
KrbSyEilxHpUdR0JS-RXFih_p4do1VBRogX74YTB37tx7z7nn_M-
59fSfPfbhLtdx4B_e3O167449ruvAsaN7XI8DD1zZ43oQuHh1j-snwO8XFlzH9i24fnPPguvx-xdcTwD3P77g-
ifgufMLrrvfXnB9A3jmnQXXXYf3ug4Ab7y-1_UW8Mef7XVt__le16Vre13XgO8uLbqOAI8AX9tYdH0dWAbWgF88vOh6A7j-
xKLrBnDgR4uujy_DvDcWXe9dgf9-dnjq6tMXps4cOcSdBU6fOsSdAV6_flj7d-
DMs4e5F4CnPznMnQKu71jiPgJO37nEfR94Abi2tsS9C_zh9BL3wLkl7l9_vsRdAC5Onr9a4l7_7RJ3Gbhx3zL3IfARsOPQMrfw0
DJ3J7AfeOXRZe6HwJEzy9yvf7TMXQXO_QfMubbMnX5nmXsGeOCDZe4h4FHgMeD4h8vcCeDwzhVuDXhh9wr3MvAK8MuF
Fe7w4gq3DPzuwAr3AbDrGyvcHuAX31nh3gRevG-Fe_z-
Fe4EcOOfV7iPgIM3VrhvAfcB23escjuAOxdXuXuAA8DRfavcMeCOb8I3YPHgKrcPOLG6yj0FPPnKKncSOHN5lXsROAt88muYf
wXG317lngFeBs4CD3-0yp3_4yp3AXhuYY07A-w7vMbtB_Z-d427F3jk2Br3L8D142vcDeDU99e47wH_-
NIa923gV2fXuKVza9wq8M7r8P-VNe5u4LfvrHHXgCO_X-OOAm-99OD0VeDd7RvT7wOv7t-Y_iGwcmBj-
n7gIvBT4OXljemlIxvTq8DRRzamjwEnH92Y_h5wDvg34JMnNqa3n9iY3gXsBpaBNeC9Jzemfwfse2pj-
h7gOvAHYPvTG9M7gUVgP_D3wL3AxZOwJ_Dt956cfvDsgvu29Z3-
vzz4hYtX79hy4idf33Lu73ZtOfnk7i3femn3llNvHfrSgR3P37rwyPrWQ0fXt-56bH3rncAdx9e3PvvU-ta3T61vffPZ9a0PP7e-
9a3n17fetf_9L-98-f0vX_rmpds_vvfS7R9cuXT7oZ1PTx3cdX7qyFPnpz4-e37q-sHXpl54_rWpu3762tQbd1-Y2r9-
YerRkxemTr5yYWpl55tT716-MvXqM7_kHn71A-7F7_zgK9pf37L6xduO3_LVr_3F9BeHQmD6z-
1OvWg7FfcgaE9_6bMXMywiI2lQvic4A79G84PhkKqtXnZeIna4RzPDNnHm081qXornWxLKGmNqG7rdCIokqQespqyQeHLct6j
54z-
```

```
dLNUgJEZpwmgkCMGRgR5GGRpiltIqNByJZqwwSpAgspR5mZc9OSbikuNgmoxpKBPpE0sZ9SwZ23IBF6IBTPNSl0SUtu4Tkb
-
Xxo7bwCirFFA2XjULahcbSiNXEHEhmPMiXs4XaipuFmewo7ZwfzY59skyiigWijcSmErFGjFUfzkfjbOiWSDFIBUveaWggXCzUM
JCI4fJZ-ZZqhvmj3XmpFPMLIGSIrslK4F76hhTu6bRZJlSWWFyRB4xAbVyEbXZTiu42XdC1FIFS1Z7SJpXWNHIIyJ702Br16firr-
CtIqBaSmGwDYTpTwBOLfQMIsoFvdi8I9NpVmBWnK_ZakoJgwxK4QxK0VIJrY0lDRVJiZjKMjCVIwiKjUSSPJhIoZEJEZmiZRMIi
kpEqIlMikpMAv5sSWHRjyqIn2IDRFq466M4GpwxIdRdNwB33dMWFMiIlKJFFOQGAzDfSjuXksKpIs4ISgoZihj4igacxfzKJ2okC4
KZY0EneuquCeUeqTeI0hM5IklM5OieWqhuh1RsUbqOFEwcUSimOIaMtgMisgyRkwulxkqj7uoS3j_QJdVHI_Q8qyBZsyIXEdNV
PYVFBRpKtiqmSjSNRX3qI9R3I9JqqAQyU-
oOKeRVEWlEIaQVME0m8yQ4IBD4khnooQGpFIngsKzNBqPC_JoTFBTq6kj0V_jazMDIaVGiCY1VWsGccIYKmYyITR985IvleK
RzIfjNdyxqOoNGZL51UIkS4iP-QJuW6Z2vBYXFEy2bTN__IXNoEdyrEEdbdRDBA86SKG2XqFNtSY0k7iUD0PQVDBydH-
pFsdOQIR3uUqZMuqCk9qOFzFHyjFH05hTmqWOznrNGG626xJ18vM0ogRRU_H60jrOBctgKB6QtIrz0TAmyei831DwoBSH8X
LfZ8CFBExMnXkfJE7Q3ZRwIcI8jKi9AARox4NxLwpPJwYXX-
QZUpotQcW2RnEuDGs4aY3ZuEStbebtE8tEwqNG0W1ppUFWQmBwbzKaZh4UKEhtrSmNFObu5c2aMkjLam2ApGpsbEvEiQ
whydv19v-iH6kspUjpBVNDTBPZIUor7YSt41Z_FGZkVvJH4_6KNGYFHzL_drKrzvh-
q6N2NRKeqfqIgYLFYBkc3jBAFQqCF5VESK1wssoQ9vZrKrI0ETnFMELyNvP85kXViRxzQjON-VFamffVYjhXqkZHJf-
gIMeQzwkrLI5GLOgtm3qwnSfqKEBE7PAh5O_PI4kINfwQIcEqKFZipgEGNqmIeOSO00JEGRdrSqIXrYLKdd00rfj0roKdcQgbM_
OQ2eOUWw-
AwogmyjRNIu2OQBWVZFuI7YJZoYIyIGdEUU6m1fJMSbdnUm7mFQctppb7XZkNtEgzhNQZOIB5mhY9ZsYKUbbNnJ9YISIe8V
P5dqP5IS95o6CJzSTkdCLYZESq5fLJ_ybnA7cKuZQRSL4WIEzxCD61KtZbblaTqwaK4xIxUT7IICmRyn2mg8QLmxL_V5t5wHi9
3Uy2dGRHQgFZzXdkCVMIjdsmXzHjxUarVIqx9DYzOxIJIH78fxeX1CQ4sjcVFwsC1Bk3eRIHOwWxIDcxTksDI1iPTMIwNVk5Tvi
Z_8fKw-5Eg7rBImIH6tLwplX_ZrKqSngS6tZTOs0GPTgYBUWXZuhMvp-Dvwp9LKL0fyUH4-
PIblaKsczskBqyyU9Gw4y3mZ5qatQuBFBEDVi-LG5DZerEWxLJDsuMKG47IUjEusIn3qiENn32uY_zgp6HIYmXRRSqk-im3nw-
v6qpvE5h_ufa1Gu3Fb0RLY2dgoIn1nx6RsonBnPthE5tETHY8fyWybCbyjFGbL7h8CkolyMoySpzmxlcqs1CeaoJkqHUbNbCtliMk
KzsZzUIUEx4pXZBGkThwvtSDbfSCIzSEMuwBiRABRLC57EUNuA1nMsouNjRJVQUpHZIrAQbOkO8EgoaYgVFA2Ghn8ctbxq
FBjMYZdyQGDgW0yOIZG0GbcDQptAaqF4Jgh3PqQKiGX6yfm2OwrqaB3e8QwHeOwKv4rIuAi5miGg2ErIste9QaCGa8ziXHG
OSKbIh3kyWV1gPZaFu6bAfSQ4SKTzwOSGMIFa5MKtrzqhGstEqzcfGuKRVOjSN3MGRMRdnZWYz5o8Y-
RJVfBYv92K8OCiB4sWFRKhtSd1cRDJ_s-
nWCovE8sguNvwg_O2SgiIJ4X4cikFabRqRHNYr6qQQQJbKvlBTQn5bkUrJKNZEEHbb54UK6tYEhAsVEZGEMqmo1RhRPBD
Vwb4Rx0VJgApo9JmQqAcjGOvpBi6kIFccVEdpiWrQZTiIJuxRqDNLyuchFnK6B4HJFWpI_bKsBjCcpdeoSySDc9RpgxuISjVoR5
BdjVG7mYbOqdYiEtaidUTj8yE4Qw_bDkEIN2GJUZja-SqoyrxQQHgOCk-TtebbMgi3FwpPsuIHhjQMJaE-
JnSRJbQAE1RfALzazcckFncPICcG-ZqMB60udEQI90cl3GJeFC2KcG6zxzK0TTNiE8lquWVIuJw26sFOViYVreK3Mn2EtpmnN-
W8AnIOt-MZ6k2CLbUWZIGzO-
wq1A1NpEMUHLULCo3bLZwa4_ZIhUj11_oWuLEdgmhpd5AvIfgnESVB5cjOBpmhtONdE3eQhovj_AzhFcEACeqqIkTSMBr9tL
GEsoCwU00h9_-oaVU-
T1UUSBYrxMIQJMhBKiijFmSMncYTCat1PxObzUSXCR_xa8WCBvE_KpEYLiTqHRAIszz5miQe9TNhb_XKTOIa0O20nVk_4dV
y0FK6dk31z-qRPBuH_NRQBAGEP-FMbLm5Txc9TZ-
MrbiNgIE_SFDMoeIZtFIf0U2S0spLQX0iEQ9tOreEPPVhq8Fk4hRCVbgLexIz2XBLspRKIqtBkQ-
CNKhjJKidVE2thBDC3YSGSTrs8Vpqoy_EcTszScucv4RUbJXSFQIyYwgYhfRJjDIKqd9hTrfKIHbneMiXbGQGmpKx11LKfeixym
kSGIw8Ws4ZiHYwIhmjmjSnKrg_6OG4PXAT3zbzIsIpISi2jbfc-if_CXDMq1zZEAAA
X-Client-Pctx: CgcSBWjR7PMq
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 05:04:56 GMT
Pragma: no-cache
Expires: -1
Cache-Control: no-cache, must-revalidate
Content-Disposition: attachment; filename="f.txt"
X-Content-Type-Options: nosniff
Content-Type: application/x-protobuffer
Content-Security-Policy: object-src 'none';base-uri 'self';script-src 'nonce-n-hvZJqLfVhm2KfZJf4QGg' 'strict-dynamic' 'report-
sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other
Permissions-Policy: unload=()
P3p: CP="This is not a P3P policy! See g.co/p3phelp for more info."
X-Goog-Zstatus: CAE
Server: gws
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
Set-Cookie: NID=519=FDK-
EYn8XqA7sgNcd9jSqI0WyMt57fA2SWEGsvSGpCutZxUe0skSs5aXztrrHsb87EWNHxu33zn6eINdmQx4Wa6UKUAIxI4hUU42
```

```
U9sSmT1bHRB-2stI4g1j75tTMXZdk6oRc94B-_OQK58a-jtFLhDEtC_vWPrie6aGmevEIv2zZA2T3aGJ1gI-L1sVHGfO;
expires=Sat, 31-May-2025 05:04:56 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=none
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

.........
```

9. Cross-domain Referer leakage

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://m.soundcloud.com**
Path:	**/12stepsapp/on-awakening/s-NVt86r3593y**

Issue detail

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

- https://m.soundcloud.com/12stepsapp/on-awakening/s-NVt86r3593y

The response contains the following links to other domains:

- https://cdn.cookielaw.org/consent/7e62c772-c97a-4d95-8d0a-f99bbeadcf61/otSDKStub.js
- https://i1.sndcdn.com/
- https://i1.sndcdn.com/avatars-Qke9HoPFUSfluy9C-OX2MVQ-t240x240.jpg
- https://i1.sndcdn.com/avatars-Qke9HoPFUSfluy9C-OX2MVQ-t500x500.jpg
- https://i2.sndcdn.com/
- https://i3.sndcdn.com/
- https://i4.sndcdn.com/
- https://m.sndcdn.com/
- https://m.sndcdn.com/_next/static/1732618350/_buildManifest.js
- https://m.sndcdn.com/_next/static/1732618350/_ssgManifest.js
- https://m.sndcdn.com/_next/static/chunks/02589dcfa436bf2fab4b0fe7d07a3cafc1e0c3eb.a5c953a6b048ac74880e.js
- https://m.sndcdn.com/_next/static/chunks/14ecde5c86bb5ff60f91cbba91cbe928858bef1b.1074ad9d9b2d95ffede8.js
- https://m.sndcdn.com/_next/static/chunks/5e631fbbbfba0e154b5a0d1f89f482de19bd32ae.f9d044a56fef6ce95140.js
- https://m.sndcdn.com/_next/static/chunks/699a3d3dcf818407f3de2f648ee2dc167a5d0087.6d41090b0b40edae7093.js
- https://m.sndcdn.com/_next/static/chunks/7d94d6b936f3df216fb39386c8cd616c58799369.3cb6f47531d9152fcda1.js
- https://m.sndcdn.com/_next/static/chunks/7d94d6b936f3df216fb39386c8cd616c58799369_CSS.118394efc85bb3e961c1.js
- https://m.sndcdn.com/_next/static/chunks/843873d166c17fb3ff01ae6a7879af3c36be5649.463626793a58a4cfbc2e.js
- https://m.sndcdn.com/_next/static/chunks/85c7519ce894131e79c3a65500314377147b6ed8.71580fb492a30fffa335.js
- https://m.sndcdn.com/_next/static/chunks/8bcfbfeaf39106fcca01cce64766cab12dc144cb.1d85ed8946dfed52f85e.js
- https://m.sndcdn.com/_next/static/chunks/8c54897ce4c59728f90778a73ca913843147ff73.a0f06b6d9eb51c3dccb1.js
- https://m.sndcdn.com/_next/static/chunks/9b7e1aab.8e63dc916312fc50802d.js
- https://m.sndcdn.com/_next/static/chunks/9e45d6ad353c0a0260d8697e6a5eecbb3912c5fa.bf6b6436bef15c0d407f.js
- https://m.sndcdn.com/_next/static/chunks/9e45d6ad353c0a0260d8697e6a5eecbb3912c5fa_CSS.2def46d8f6d9630e1283.js
- https://m.sndcdn.com/_next/static/chunks/9fb0f57048489bcb80dcebe394ed9475d8c8fb16.0cdc7ddd40ede533b2e6.js
- https://m.sndcdn.com/_next/static/chunks/a0a91107783630a1b4c90503be1b6ecc636be72a.6e24ae925b27b7567f6e.js
- https://m.sndcdn.com/_next/static/chunks/a87222b1e467548e0d388034bdebeba2f0f26bb6.c51952f6b283f101df39.js
- https://m.sndcdn.com/_next/static/chunks/b2f6b0aaded67297dd4329f5d11f4f395db1d6f2.d12904000f5b9a38e17a.js
- https://m.sndcdn.com/_next/static/chunks/bfbb44f9390276dbd6452c1dd4ff5e47d2f275c8.4f5e44be1d88995ed3d2.js
- https://m.sndcdn.com/_next/static/chunks/c32e057f4d02dbc1f5b44cd40b5e7d23fc6e81ec.58b72375c75190232ffd.js
- https://m.sndcdn.com/_next/static/chunks/ce0d8553f12fb8f106751d612d6ac32b06258698.99c3931abdaa9656d4bd.js
- https://m.sndcdn.com/_next/static/chunks/commons.cb9462d91ed8ef693344.js
- https://m.sndcdn.com/_next/static/chunks/d617f59ed564c0393c29c29090c7504aff36450f.4276e24c7a1bafc9e62c.js

- https://m.sndcdn.com/_next/static/chunks/d764dcb2.c0256cb3828a8a47ad69.js
- https://m.sndcdn.com/_next/static/chunks/da41d81fc5383ee5afd948a53479347c2eb390a3.52ad18c03f1b024133d1.js
- https://m.sndcdn.com/_next/static/chunks/ebed66cde64134a45e4e51e30597be478f11b8f8.c0cbbbb321ac7517bc1a.js
- https://m.sndcdn.com/_next/static/chunks/f70ca7d87a0fcf7a353c3b52800b8f6e86389c81.b1352bf601fc44c7bf0c.js
- https://m.sndcdn.com/_next/static/chunks/f9f25f7cabbd26d7943b2708ec319b8cfd7f68fd.86b149a8fbb66c997a6b.js
- https://m.sndcdn.com/_next/static/chunks/ffd80846.4976c0dc2ec31aff9501.js
- https://m.sndcdn.com/_next/static/chunks/main-d39e36461395347a8b66.js
- https://m.sndcdn.com/_next/static/chunks/pages/[user]/[track]/[secretToken]-aebf0334744012058c2d.js
- https://m.sndcdn.com/_next/static/chunks/pages/_app-ac0480d10c35ae08406e.js
- https://m.sndcdn.com/_next/static/chunks/polyfills-65148f4d99d0e06c1fd8.js
- https://m.sndcdn.com/_next/static/chunks/webpack-4f65844e3fc8e15936bb.js
- https://m.sndcdn.com/_next/static/css/13c91a587d9631c01212.css
- https://m.sndcdn.com/_next/static/css/32ac4681726a69bdbbb0.css
- https://m.sndcdn.com/_next/static/css/5d23c0a7f12b04a452bb.css
- https://m.sndcdn.com/_next/static/css/f9cb2605eefcbf16430c.css
- https://m.sndcdn.com/_next/static/images/English-2c0ad42774f0308a9762d7184607bb73.png
- https://m.sndcdn.com/_next/static/images/apple-touch-icon-120-810d80d153fe7629e01c78e25c021747.png
- https://m.sndcdn.com/_next/static/images/apple-touch-icon-180-893d0d532e8fbba714cceb8d9eae9567.png
- https://m.sndcdn.com/_next/static/images/favicon-16-b8c7cd12bb1f82f55f785072ad6c2138.png
- https://m.sndcdn.com/_next/static/images/favicon-32-7c86406588c8fb13cb11b779c7ebe9eb.png
- https://securepubads.g.doubleclick.net/tag/js/gpt.js
- https://style.sndcdn.com/
- https://style.sndcdn.com/fonts/soundcloud-sans-500-cf1a3e1fb4cee50fe430b572d2c855b4.woff2
- https://style.sndcdn.com/fonts/soundcloud-sans-700-4d19511ea677f5ec5c828f0258549ec4.woff2
- https://style.sndcdn.com/fonts/soundcloud-sans-900-03bbceefe9659e9d9cee10e885a88dc2.woff2
- https://w1.sndcdn.com/
- https://wis.sndcdn.com/

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 /12stepsapp/on-awakening/s-NVt86r3593y?
si=1d284dff98974cb183c9f96d537444f1&utm_source=clipboard&utm_medium=text&utm_campaign=social_sharing HTTP/1.1
Host: m.soundcloud.com
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
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.twelve_steps.twelve_steps
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
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: sc_anonymous_id=585810-837106-950987-811574; path=/; expires=Mon, 27 Nov 2034 05:09:33 GMT;
domain=.soundcloud.com
Cache-Control: private, max-age=0, no-cache, no-store
Content-Security-Policy: frame-ancestors 'none';
X-Frame-Options: DENY
Referrer-Policy: never, no-referrer
X-Content-Type-Options: nosniff
Feature-Policy: accelerometer none; ambient-light-sensor none; autoplay none; battery none; camera none; display-capture
none; document-domain none; fullscreen none; geolocation none; gyroscope none; magnetometer none; microphone none;
midi none; picture-in-picture none; sync-xhr none; usb none; wake-lock none
Etag: "1130d-1zKjkhWHDWpKdwW365h9bK5qCko"
Date: Fri, 29 Nov 2024 05:09:33 GMT
Strict-Transport-Security: max-age=63072000
Server: am/2
Vary: Accept,Accept-Encoding,Accept-Language,Origin
X-Cache: Miss from cloudfront
Via: 1.1 ea419f8269940bd7231c70acd36c430c.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: 47mt75G32Scs3bIIcMxSZt79zPma0WQT_Gu3EHMfx4JnII-ltzUOSA==

<!DOCTYPE html><html lang="en" style="min-width:fit-content"><head><script>
(function () {
window.ddjskey = '7FC6D561817844F25B65CDD97F28A1';
window.ddoptions =
...[SNIP]...
</style><script src="https://cdn.cookielaw.org/consent/7e62c772-c97a-4d95-8d0a-f99bbeadcf61/otSDKStub.js"
type="text/javascript" data-domain-script="7e62c772-c97a-4d95-8d0a-f99bbeadcf61" data-testid="ot-script"></script>
...[SNIP]...
<link rel="author" href="/12stepsapp"/><link rel="preload" as="image" href="https://i1.sndcdn.com/avatars-
Qke9HoPFUSfIuy9C-OX2MVQ-t500x500.jpg"/><link rel="preload"
href="https://m.sndcdn.com/_next/static/css/32ac4681726a69bdbbb0.css" as="style"/>
...[SNIP]...
<div class="HeroImage_HeroImageContainer__1tPh-" style="padding-bottom:100%"><img src="https://i1.sndcdn.com/avatars-
Qke9HoPFUSfIuy9C-OX2MVQ-t500x500.jpg" class="" alt="On Awakening"/></div>
...[SNIP]...
<picture><img class="Artwork_ArtworkImage__1Ws9- Artwork_CircularArtwork__rfVyb" alt="12Steps.app"
src="https://i1.sndcdn.com/avatars-Qke9HoPFUSfIuy9C-OX2MVQ-t240x240.jpg" data-testid="actual-image"/></picture>
...[SNIP]...
```

```
tm_campaign=social_sharing&amp;mt=8&amp;at=direct&amp;pt=mobi&amp;ct=social_sharing" target="_blank" rel="nofollow
noreferrer" data-testid="open-in-store-link" class="StoreLink_StoreLinkButton__3_Qd3"><img data-testid="android-banner"
class="StoreLink_StoreLinkBanner__20xNz" src="https://m.sndcdn.com/_next/static/images/English-
2c0ad42774f0308a9762d7184607bb73.png" alt="Google Play Link"/></a>
```

...[SNIP]...

```
</script><script nomodule="" src="https://m.sndcdn.com/_next/static/chunks/polyfills-65148f4d99d0e06c1fd8.js"></script>
<script src="https://m.sndcdn.com/_next/static/chunks/main-d39e36461395347a8b66.js" async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/webpack-4f65844e3fc8e15936bb.js" async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/ffd80846.4976c0dc2ec31aff9501.js" async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/9b7e1aab.8e63dc916312fc50802d.js" async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/d764dcb2.c0256cb3828a8a47ad69.js" async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/commons.cb9462d91ed8ef693344.js" async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/14ecde5c86bb5ff60f91cbba91cbe928858bef1b.1074ad9d9b2d95ffede8.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/699a3d3dcf818407f3de2f648ee2dc167a5d0087.6d41090b0b40edae7093.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/ce0d8553f12fb8f106751d612d6ac32b06258698.99c3931abdaa9656d4bd.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/c32e057f4d02dbc1f5b44cd40b5e7d23fc6e81ec.58b72375c75190232ffd.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/9fb0f57048489bcb80dcebe394ed9475d8c8fb16.0cdc7ddd40ede533b2e6.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/8bcfbfeaf39106fcca01cce64766cab12dc144cb.1d85ed8946dfed52f85e.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/a87222b1e467548e0d388034bdebeba2f0f26bb6.c51952f6b283f101df39.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/b2f6b0aaded67297dd4329f5d11f4f395db1d6f2.d12904000f5b9a38e17a.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/ebed66cde64134a45e4e51e30597be478f11b8f8.c0cbbbb321ac7517bc1a.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/f9f25f7cabbd26d7943b2708ec319b8cfd7f68fd.86b149a8fbb66c997a6b.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/7d94d6b936f3df216fb39386c8cd616c58799369.3cb6f47531d9152fcda1.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/7d94d6b936f3df216fb39386c8cd616c58799369_CSS.118394efc85bb3e961c1.j
s" async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/5e631fbbbfba0e154b5a0d1f89f482de19bd32ae.f9d044a56fef6ce95140.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/f70ca7d87a0fcf7a353c3b52800b8f6e86389c81.b1352bf601fc44c7bf0c.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/843873d166c17fb3ff01ae6a7879af3c36be5649.463626793a58a4cfbc2e.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/da41d81fc5383ee5afd948a53479347c2eb390a3.52ad18c03f1b024133d1.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/a0a91107783630a1b4c90503be1b6ecc636be72a.6e24ae925b27b7567f6e.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/d617f59ed564c0393c29c29090c7504aff36450f.4276e24c7a1bafc9e62c.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/8c54897ce4c59728f90778a73ca913843147ff73.a0f06b6d9eb51c3dccb1.js"
async=""></script><script src="https://m.sndcdn.com/_next/static/chunks/pages/_app-ac0480d10c35ae08406e.js" async="">
</script><script
src="https://m.sndcdn.com/_next/static/chunks/85c7519ce894131e79c3a65500314377147b6ed8.71580fb492a30fffa335.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/bfbb44f9390276dbd6452c1dd4ff5e47d2f275c8.4f5e44be1d88995ed3d2.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/9e45d6ad353c0a0260d8697e6a5eecbb3912c5fa.bf6b6436bef15c0d407f.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/9e45d6ad353c0a0260d8697e6a5eecbb3912c5fa_CSS.2def46d8f6d9630e1283
.js" async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/02589dcfa436bf2fab4b0fe7d07a3cafc1e0c3eb.a5c953a6b048ac74880e.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/pages/%5Buser%5D/%5Btrack%5D/%5BsecretToken%5D-
aebf0334744012058c2d.js" async=""></script><script src="https://m.sndcdn.com/_next/static/1732618350/_buildManifest.js"
async=""></script><script src="https://m.sndcdn.com/_next/static/1732618350/_ssgManifest.js" async=""></script>
```

...[SNIP]...

10. Cross-domain script include

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://m.soundcloud.com**
Path:	**/12stepsapp/on-awakening/s-NVt86r3593y**

Issue detail

The response dynamically includes the following scripts from other domains:

- https://cdn.cookielaw.org/consent/7e62c772-c97a-4d95-8d0a-f99bbeadcf61/otSDKStub.js
- https://m.sndcdn.com/_next/static/1732618350/_buildManifest.js
- https://m.sndcdn.com/_next/static/1732618350/_ssgManifest.js
- https://m.sndcdn.com/_next/static/chunks/02589dcfa436bf2fab4b0fe7d07a3cafc1e0c3eb.a5c953a6b048ac74880e.js
- https://m.sndcdn.com/_next/static/chunks/14ecde5c86bb5ff60f91cbba91cbe928858bef1b.1074ad9d9b2d95ffede8.js
- https://m.sndcdn.com/_next/static/chunks/5e631fbbbfba0e154b5a0d1f89f482de19bd32ae.f9d044a56fef6ce95140.js
- https://m.sndcdn.com/_next/static/chunks/699a3d3dcf818407f3de2f648ee2dc167a5d0087.6d41090b0b40edae7093.js
- https://m.sndcdn.com/_next/static/chunks/7d94d6b936f3df216fb39386c8cd616c58799369.3cb6f47531d9152fcda1.js
- https://m.sndcdn.com/_next/static/chunks/7d94d6b936f3df216fb39386c8cd616c58799369_CSS.118394efc85bb3e961c1.js
- https://m.sndcdn.com/_next/static/chunks/843873d166c17fb3ff01ae6a7879af3c36be5649.463626793a58a4cfbc2e.js
- https://m.sndcdn.com/_next/static/chunks/85c7519ce894131e79c3a65500314377147b6ed8.71580fb492a30fffa335.js
- https://m.sndcdn.com/_next/static/chunks/8bcfbfeaf39106fcca01cce64766cab12dc144cb.1d85ed8946dfed52f85e.js
- https://m.sndcdn.com/_next/static/chunks/8c54897ce4c59728f90778a73ca913843147ff73.a0f06b6d9eb51c3dccb1.js
- https://m.sndcdn.com/_next/static/chunks/9b7e1aab.8e63dc916312fc50802d.js
- https://m.sndcdn.com/_next/static/chunks/9e45d6ad353c0a0260d8697e6a5eecbb3912c5fa.bf6b6436bef15c0d407f.js
- https://m.sndcdn.com/_next/static/chunks/9e45d6ad353c0a0260d8697e6a5eecbb3912c5fa_CSS.2def46d8f6d9630e1283.js
- https://m.sndcdn.com/_next/static/chunks/9fb0f57048489bcb80dcebe394ed9475d8c8fb16.0cdc7ddd40ede533b2e6.js
- https://m.sndcdn.com/_next/static/chunks/a0a91107783630a1b4c90503be1b6ecc636be72a.6e24ae925b27b7567f6e.js
- https://m.sndcdn.com/_next/static/chunks/a87222b1e467548e0d388034bdebeba2f0f26bb6.c51952f6b283f101df39.js
- https://m.sndcdn.com/_next/static/chunks/b2f6b0aaded67297dd4329f5d11f4f395db1d6f2.d12904000f5b9a38e17a.js
- https://m.sndcdn.com/_next/static/chunks/bfbb44f9390276dbd6452c1dd4ff5e47d2f275c8.4f5e44be1d88995ed3d2.js
- https://m.sndcdn.com/_next/static/chunks/c32e057f4d02dbc1f5b44cd40b5e7d23fc6e81ec.58b72375c75190232ffd.js
- https://m.sndcdn.com/_next/static/chunks/ce0d8553f12fb8f106751d612d6ac32b06258698.99c3931abdaa9656d4bd.js
- https://m.sndcdn.com/_next/static/chunks/commons.cb9462d91ed8ef693344.js
- https://m.sndcdn.com/_next/static/chunks/d617f59ed564c0393c29c29090c7504aff36450f.4276e24c7a1bafc9e62c.js
- https://m.sndcdn.com/_next/static/chunks/d764dcb2.c0256cb3828a8a47ad69.js
- https://m.sndcdn.com/_next/static/chunks/da41d81fc5383ee5afd948a53479347c2eb390a3.52ad18c03f1b024133d1.js
- https://m.sndcdn.com/_next/static/chunks/ebed66cde64134a45e4e51e30597be478f11b8f8.c0cbbbb321ac7517bc1a.js
- https://m.sndcdn.com/_next/static/chunks/f70ca7d87a0fcf7a353c3b52800b8f6e86389c81.b1352bf601fc44c7bf0c.js
- https://m.sndcdn.com/_next/static/chunks/f9f25f7cabbd26d7943b2708ec319b8cfd7f68fd.86b149a8fbb66c997a6b.js
- https://m.sndcdn.com/_next/static/chunks/ffd80846.4976c0dc2ec31aff9501.js
- https://m.sndcdn.com/_next/static/chunks/main-d39e36461395347a8b66.js
- https://m.sndcdn.com/_next/static/chunks/pages/[user]/[track]/[secretToken]-aebf0334744012058c2d.js
- https://m.sndcdn.com/_next/static/chunks/pages/_app-ac0480d10c35ae08406e.js
- https://m.sndcdn.com/_next/static/chunks/polyfills-65148f4d99d0e06c1fd8.js
- https://m.sndcdn.com/_next/static/chunks/webpack-4f65844e3fc8e15936bb.js
- https://securepubads.g.doubleclick.net/tag/js/gpt.js

Issue background

When an application includes a script from an external domain, this script is executed by the browser within the security context of the invoking application. The script can therefore do anything that the application's own scripts can do, such as accessing application data and performing actions within the context of the current user.

If you include a script from an external domain, then you are trusting that domain with the data and functionality of your application, and you are trusting the domain's own security to prevent an attacker from modifying the script to perform malicious actions within your application.

Issue remediation

Scripts should ideally not be included from untrusted domains. Applications that rely on static third-party scripts should consider using Subresource Integrity to make browsers verify them, or copying the contents of these scripts onto their own domain and including them from there. If that is not possible (e.g. for licensing reasons) then consider reimplementing the script's functionality within application code.

References

- Subresource Integrity

Vulnerability classifications

- CWE-829: Inclusion of Functionality from Untrusted Control Sphere

Request

```
GET /12stepsapp/on-awakening/s-NVt86r3593y?
si=1d284dff98974cb183c9f96d537444f1&utm_source=clipboard&utm_medium=text&utm_campaign=social_sharing HTTP/1.1
Host: m.soundcloud.com
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
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.twelve_steps.twelve_steps
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
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: sc_anonymous_id=585810-837106-950987-811574; path=/; expires=Mon, 27 Nov 2034 05:09:33 GMT;
domain=.soundcloud.com
Cache-Control: private, max-age=0, no-cache, no-store
Content-Security-Policy: frame-ancestors 'none';
X-Frame-Options: DENY
Referrer-Policy: never, no-referrer
X-Content-Type-Options: nosniff
Feature-Policy: accelerometer none; ambient-light-sensor none; autoplay none; battery none; camera none; display-capture
none; document-domain none; fullscreen none; geolocation none; gyroscope none; magnetometer none; microphone none;
midi none; picture-in-picture none; sync-xhr none; usb none; wake-lock none
Etag: "1130d-1zKjkhWHDWpKdwW365h9bK5qCko"
Date: Fri, 29 Nov 2024 05:09:33 GMT
Strict-Transport-Security: max-age=63072000
Server: am/2
Vary: Accept,Accept-Encoding,Accept-Language,Origin
X-Cache: Miss from cloudfront
Via: 1.1 ea419f8269940bd7231c70acd36c430c.cloudfront.net (CloudFront)
```

```
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: 47mt75G32Scs3bIIcMxSZt79zPma0WQT_Gu3EHMfx4JnII-ltzUOSA==

<!DOCTYPE html><html lang="en" style="min-width:fit-content"><head><script>
(function () {
window.ddjskey = '7FC6D561817844F25B65CDD97F28A1';
window.ddoptions =
...[SNIP]...
</style><script src="https://cdn.cookielaw.org/consent/7e62c772-c97a-4d95-8d0a-f99bbeadcf61/otSDKStub.js"
type="text/javascript" data-domain-script="7e62c772-c97a-4d95-8d0a-f99bbeadcf61" data-testid="ot-script"></script>
...[SNIP]...
</script><script nomodule="" src="https://m.sndcdn.com/_next/static/chunks/polyfills-65148f4d99d0e06c1fd8.js"></script>
<script src="https://m.sndcdn.com/_next/static/chunks/main-d39e36461395347a8b66.js" async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/webpack-4f65844e3fc8e15936bb.js" async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/ffd80846.4976c0dc2ec31aff9501.js" async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/9b7e1aab.8e63dc916312fc50802d.js" async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/d764dcb2.c0256cb3828a8a47ad69.js" async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/commons.cb9462d91ed8ef693344.js" async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/14ecde5c86bb5ff60f91cbba91cbe928858bef1b.1074ad9d9b2d95ffede8.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/699a3d3dcf818407f3de2f648ee2dc167a5d0087.6d41090b0b40edae7093.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/ce0d8553f12fb8f106751d612d6ac32b06258698.99c3931abdaa9656d4bd.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/c32e057f4d02dbc1f5b44cd40b5e7d23fc6e81ec.58b72375c75190232ffd.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/9fb0f57048489bcb80dcebe394ed9475d8c8fb16.0cdc7ddd40ede533b2e6.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/8bcfbfeaf39106fcca01cce64766cab12dc144cb.1d85ed8946dfed52f85e.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/a87222b1e467548e0d388034bdebeba2f0f26bb6.c51952f6b283f101df39.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/b2f6b0aaded67297dd4329f5d11f4f395db1d6f2.d12904000f5b9a38e17a.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/ebed66cde64134a45e4e51e30597be478f11b8f8.c0cbbbb321ac7517bc1a.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/f9f25f7cabbd26d7943b2708ec319b8cfd7f68fd.86b149a8fbb66c997a6b.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/7d94d6b936f3df216fb39386c8cd616c58799369.3cb6f47531d9152fcda1.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/7d94d6b936f3df216fb39386c8cd616c58799369_CSS.118394efc85bb3e961c1.j
s" async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/5e631fbbbfba0e154b5a0d1f89f482de19bd32ae.f9d044a56fef6ce95140.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/f70ca7d87a0fcf7a353c3b52800b8f6e86389c81.b1352bf601fc44c7bf0c.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/843873d166c17fb3ff01ae6a7879af3c36be5649.463626793a58a4cfbc2e.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/da41d81fc5383ee5afd948a53479347c2eb390a3.52ad18c03f1b024133d1.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/a0a91107783630a1b4c90503be1b6ecc636be72a.6e24ae925b27b7567f6e.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/d617f59ed564c0393c29c29090c7504aff36450f.4276e24c7a1bafc9e62c.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/8c54897ce4c59728f90778a73ca913843147ff73.a0f06b6d9eb51c3dccb1.js"
async=""></script><script src="https://m.sndcdn.com/_next/static/chunks/pages/_app-ac0480d10c35ae08406e.js" async="">
</script><script
src="https://m.sndcdn.com/_next/static/chunks/85c7519ce894131e79c3a65500314377147b6ed8.71580fb492a30fffa335.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/bfbb44f9390276dbd6452c1dd4ff5e47d2f275c8.4f5e44be1d88995ed3d2.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/9e45d6ad353c0a0260d8697e6a5eecbb3912c5fa.bf6b6436bef15c0d407f.js"
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/9e45d6ad353c0a0260d8697e6a5eecbb3912c5fa_CSS.2def46d8f6d9630e1283
.js" async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/02589dcfa436bf2fab4b0fe7d07a3cafc1e0c3eb.a5c953a6b048ac74880e.js"
```

```
async=""></script><script
src="https://m.sndcdn.com/_next/static/chunks/pages/%5Buser%5D/%5Btrack%5D/%5BsecretToken%5D-
aebf0334744012058c2d.js" async=""></script><script src="https://m.sndcdn.com/_next/static/1732618350/_buildManifest.js"
async=""></script><script src="https://m.sndcdn.com/_next/static/1732618350/_ssgManifest.js" async=""></script>
...[SNIP]...
```

11. Cookie without HttpOnly flag set

There are 2 instances of this issue:

- https://m.soundcloud.com/12stepsapp/on-awakening/s-NVt86r3593y
- https://securepubads.g.doubleclick.net/pagead/ppub_config

Issue background

If the HttpOnly attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This measure makes certain client-side attacks, such as cross-site scripting, slightly harder to exploit by preventing them from trivially capturing the cookie's value via an injected script.

Issue remediation

There is usually no good reason not to set the HttpOnly flag on all cookies. Unless you specifically require legitimate client-side scripts within your application to read or set a cookie's value, you should set the HttpOnly flag by including this attribute within the relevant Set-cookie directive.

You should be aware that the restrictions imposed by the HttpOnly flag can potentially be circumvented in some circumstances, and that numerous other serious attacks can be delivered by client-side script injection, aside from simple cookie stealing.

References

- Web Security Academy: Exploiting XSS vulnerabilities
- HttpOnly effectiveness

Vulnerability classifications

- CWE-16: Configuration
- CAPEC-31: Accessing/Intercepting/Modifying HTTP Cookies

11.1. https://m.soundcloud.com/12stepsapp/on-awakening/s-NVt86r3593y

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://m.soundcloud.com**
Path:	**/12stepsapp/on-awakening/s-NVt86r3593y**

Issue detail

The following cookie was issued by the application and does not have the HttpOnly flag set:

- sc_anonymous_id

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.

Request

```
GET /12stepsapp/on-awakening/s-NVt86r3593y?
si=1d284dff98974cb183c9f96d537444f1&utm_source=clipboard&utm_medium=text&utm_campaign=social_sharing HTTP/1.1
Host: m.soundcloud.com
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
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.twelve_steps.twelve_steps
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
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: sc_anonymous_id=585810-837106-950987-811574; path=/; expires=Mon, 27 Nov 2034 05:09:33 GMT;
domain=.soundcloud.com
Cache-Control: private, max-age=0, no-cache, no-store
Content-Security-Policy: frame-ancestors 'none';
X-Frame-Options: DENY
Referrer-Policy: never, no-referrer
X-Content-Type-Options: nosniff
Feature-Policy: accelerometer none; ambient-light-sensor none; autoplay none; battery none; camera none; display-capture
none; document-domain none; fullscreen none; geolocation none; gyroscope none; magnetometer none; microphone none;
midi none; picture-in-picture none; sync-xhr none; usb none; wake-lock none
Etag: "1130d-1zKjkhWHDWpKdwW365h9bK5qCko"
Date: Fri, 29 Nov 2024 05:09:33 GMT
Strict-Transport-Security: max-age=63072000
Server: am/2
Vary: Accept,Accept-Encoding,Accept-Language,Origin
X-Cache: Miss from cloudfront
Via: 1.1 ea419f8269940bd7231c70acd36c430c.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: 47mt75G32Scs3bIIcMxSZt79zPma0WQT_Gu3EHMfx4JnII-ltzUOSA==

<!DOCTYPE html><html lang="en" style="min-width:fit-content"><head><script>
(function () {
window.ddjskey = '7FC6D561817844F25B65CDD97F28A1';
window.ddoptions =
...[SNIP]...
```

11.2. https://securepubads.g.doubleclick.net/pagead/ppub_config

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://securepubads.g.doubleclick.net**
Path:	**/pagead/ppub_config**

Issue detail

The following cookie was issued by the application and does not have the HttpOnly flag set:

- test_cookie

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.

Request

```
GET /pagead/ppub_config?ippd=m.soundcloud.com HTTP/2
Host: securepubads.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
Accept: */*
Origin: https://m.soundcloud.com
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://m.soundcloud.com/
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
Access-Control-Allow-Origin: *
Date: Fri, 29 Nov 2024 05:09:59 GMT
Expires: Fri, 29 Nov 2024 05:09:59 GMT
Cache-Control: private, max-age=3600, stale-while-revalidate=3600
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Server: cafe
Content-Length: 2466
X-Xss-Protection: 0
Set-Cookie: test_cookie=CheckForPermission; expires=Fri, 29-Nov-2024 05:24:59 GMT; path=/; domain=.doubleclick.net; Secure; SameSite=none
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

```
[["soundcloud.com",null,"m.soundcloud.com",null,null,["115535218"]],[],[],null,null,[["115535218",
[["liveintent.indexexchange.com",null,1],["openx.net",null,1],["uidapi.com",null,1],["id5-sync.com",nu
...[SNIP]...
```

12. Browser cross-site scripting filter disabled

There are 6 instances of this issue:

- https://app-measurement.com/config/app/1:414843287017:android:9d526f6607903f60
- https://app-measurement.com/config/app/1:551011954849:android:c927b6ed30ba0123
- https://inbox.google.com/sync/el2
- https://securepubads.g.doubleclick.net/pagead/managed/js/gpt/m202411180101/pubads_impl.js
- https://securepubads.g.doubleclick.net/pagead/ppub_config
- https://securepubads.g.doubleclick.net/tag/js/gpt.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)

12.1. https://app-measurement.com/config/app/1:414843287017:android:9d526f6607903f60

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app-measurement.com**
Path:	**/config/app/1:414843287017:android:9d526f6607903f60**

Request

```
GET /config/app/1:414843287017:android:9d526f6607903f60?gmp_version=244534&runtime_version=0&platform=android
HTTP/2
Host: app-measurement.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
Etag: 17195220862225793570
Content-Type: application/x-protobuf
Cross-Origin-Resource-Policy: cross-origin
Content-Security-Policy-Report-Only: script-src 'none'; form-action 'none'; frame-src 'none'; report-uri
https://csp.withgoogle.com/csp/scaffolding/ascgcycc:941:0
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=coop_reporting
Report-To: {"group":"coop_reporting","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-
to/scaffolding/ascgcycc:941:0"}],}
Date: Fri, 29 Nov 2024 05:05:37 GMT
Server: Google Tag Manager
Content-Length: 51671
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

..........'1:414843287017:android:9d526f6607903f60.."%
.measurement.audience.max_count..400"4
-measurement.upload.max_public_user_properties..100"5
-measurement.upload.max_event_name_cardinality..2000
...[SNIP]...
```

12.2. https://app-measurement.com/config/app/1:551011954849:android:c927b6ed30ba0123

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app-measurement.com**
Path:	**/config/app/1:551011954849:android:c927b6ed30ba0123**

Request

```
GET /config/app/1:551011954849:android:c927b6ed30ba0123?gmp_version=244534&runtime_version=0&platform=android
HTTP/2
Host: app-measurement.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
Etag: 16786314539300445072
Content-Type: application/x-protobuf
Cross-Origin-Resource-Policy: cross-origin
Content-Security-Policy-Report-Only: script-src 'none'; form-action 'none'; frame-src 'none'; report-uri
https://csp.withgoogle.com/csp/scaffolding/ascgcycc:941:0
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=coop_reporting
Report-To: {"group":"coop_reporting","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-
to/scaffolding/ascgcycc:941:0"}],}
Date: Fri, 29 Nov 2024 05:05:27 GMT
Server: Google Tag Manager
Content-Length: 28576
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

..........'1:551011954849:android:c927b6ed30ba0123.."%
.measurement.audience.max_count..400"4
-measurement.upload.max_public_user_properties..100"5
-measurement.upload.max_event_name_cardinality..2000
...[SNIP]...
```

12.3. https://inbox.google.com/sync/el2

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://inbox.google.com**
Path:	**/sync/el2**

Request

```
POST /sync/el2?hl=en_US&c=0 HTTP/2
Host: inbox.google.com
X-Google-Btd: 1
X-Gmail-Btai:
GswBMABQAWgBeAGAAQGIAQGQAQCYAQGwAQC4AQHAAQHIAQHQAQHYAQDgAQHoAQHwAQH4AQCAAgCIAgCQAg
GYAgCgAgCqAgJlbrICSkFuZHJvaWQtR21haWwvNjIxOTY3NzIgKHN3NDExZHA7IDQyMGRwaSkgKGdlbmVyaWNfeDg2X2F
ybSBSU1IxLjIwMTAxMy4wMDEpwAIAyAIZ0AIA2AIA4AIA6AIA8AIA+AIBgAMBiAMBkAMAmAMAoAMAqAMBsAMAuAMAwAM
AyAMA0AMAOBtCHDIwMjAuMDUuMTcuMzEyNjc5MTIxLnJlbGVhc2VlAIACWhVHb29nbGUgc2RrX2dwaG9uZV94ODZggK+1
9///////AWoQQW1lcmljYS9OZXdfWW9ya3ABgAGkmNQdigEAkgEWZWFfSlEyNjZUQzJPUkhlTVRHR21pQ5gBxeLSsrcy
User-Agent: Android-Gmail/62196772 (sw411dp; 420dpi) (generic_x86_arm RSR1.201013.001)
```

```
Authorization: OAuth
ya29.a0AeDClZDjxSKYIpaYmaJyL0A8u6Rk1H_iWNx3XmKAIfFKXzndBSFaIUJrfICX5aYuRXYxjeBiPMV8Kb1BdTXWIn9mEYk
ByoWZw4rjrk76InRgqSK-JMSN9Gx9WaXeCy1S6K4q-
0NcsYGmPUiwTdvHimhlUZH4dMgulhjQEwJQqEhDfTh8J2VzFJ05IftOUgBIYtgroSSOPJzzsw7wpULNYagiOiBISIZo-
rrbKL2viiqwyxFMVobO_H4ByfpCSwmQ43fypZf5JiwhWnH1n6WEt7NZSv_3TVfnMr9AzpFy0Tz7KBXXCmhVkI8AeWWXvIrzV1
wbDTi7zOAf_IRu-GJ1YMgxVEv2aCgYKAWsSARISFQHGX2MiqzslycKAiTnTx474LvBsrg0355
Content-Type: application/x-protobuf
Accept-Encoding: gzip, deflate, br
Content-Length: 77


K
....
../.......
9..B5    ..'    e7yB..P.Ke7yB..../!.......?(.8./..../!.......?(.
```

Response

```
HTTP/2 200 OK
Content-Type: application/vnd.google.octet-stream-compressible
Vary: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site
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 05:11:22 GMT
Content-Disposition: attachment; filename="response.bin"; filename*=UTF-8''response.bin
X-Content-Type-Options: nosniff
P3p: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Cross-Origin-Opener-Policy: same-origin-allow-popups
X-Goog-Server-Latency: 28
Gfe-Rtt-Ms: 151
Server: ESF
Content-Length: 0
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
Set-Cookie: NID=519=NB8YrHSbvrKWZwigCjAB3yLIApkLZeeBKXMBUbct9-QI722_QTnujD-aRT_1d-
1Gk0WjGNLhQPnr2mggCRXmAX2Lmyc5cxhp8BRxqWpwddXHSf1b1jp08tweHHEuMesh1uI7LDGLYf82WYHFMIQMABWA2o
XVkRYSvUfPV6no3UfDDLXP0g; expires=Sat, 31-May-2025 05:11:22 GMT; path=/; domain=.google.com; HttpOnly
Set-Cookie: COMPASS=bigtop-
sync=CsMBAAlriVc4UX9z0cAzW1FV_kTljjHKDBYww6QwK1BbFGoDPn1cA4W1_atRww7avYD77iwqHfssRkTd3qMNYn2nz3
1b5FmUX8mtCSNWDZuIogdCwcJhUdTstub4huvkkqXdamHk9Qo587TmbgLAsVriWzQdamY9REAuy3mLC1K465M-
yPBN7aR1_oJTQzpjyFRTIX850rRARWctV_HiWbh6Tz4VJHw7nqIp1JVg8nGtrdDS_HnnH4hptHAjze1CvD49DyIGELS6qroGG
uoBAAlriVdBttfLFoiCZoTZ1zEiZ4nebYMjvltBpLKTF403lHEdt1auE0Xbfc7hMJf_5f508MVTN7dvnJnxQHGaXLhEB_mzPADs-
lDQ4Aw8oti60DUlIqKqgWwnvkco9dsQhBu8i9OHfroe9lbOD8v6nlgK8zsqt8H8M5K0Z-7JmW-
quxGF1XidTRh14TcFR0nx_bO8htQWfJ_Lgb5a7eDT6DzmMGEYObCnimihnQP7YfPfUDALV6xXmpPvCu4KhVBJgpkaqeZo0E
PddZqiN7DkmgLIIH9LNplD-SsGEGK-HOeczLO69tJ5JMCvMAE; expires=Mon, 09-Dec-2024 05:11:22 GMT; path=/sync;
Secure; HttpOnly
Alt-Svc: clear
```

12.4. https://securepubads.g.doubleclick.net/pagead/managed/js/gpt/m202411180101/pubads_impl.js

Summary

Severity:	**Information**
Confidence:	**Certain**

Host:	**https://securepubads.g.doubleclick.net**
Path:	**/pagead/managed/js/gpt/m202411180101/pubads_impl.js**

Request

```
GET /pagead/managed/js/gpt/m202411180101/pubads_impl.js HTTP/2
Host: securepubads.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
Accept: */*
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://m.soundcloud.com/
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
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Server: cafe
Content-Length: 503686
X-Xss-Protection: 0
Date: Thu, 28 Nov 2024 05:32:56 GMT
Expires: Fri, 28 Nov 2025 05:32:56 GMT
Cache-Control: public, immutable, max-age=31536000
Age: 85000
Etag: 1421939719645060458
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 Google LLC
SPDX-License-Identifier: Apache-2.0
*/
/*


Copyright (c) 2015
...[SNIP]...
```

12.5. https://securepubads.g.doubleclick.net/pagead/ppub_config

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://securepubads.g.doubleclick.net**
Path:	**/pagead/ppub_config**

Request

```
GET /pagead/ppub_config?ippd=m.soundcloud.com HTTP/2
Host: securepubads.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
Accept: */*
Origin: https://m.soundcloud.com
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://m.soundcloud.com/
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
Access-Control-Allow-Origin: *
Date: Fri, 29 Nov 2024 05:09:59 GMT
Expires: Fri, 29 Nov 2024 05:09:59 GMT
Cache-Control: private, max-age=3600, stale-while-revalidate=3600
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Server: cafe
Content-Length: 2466
X-Xss-Protection: 0
Set-Cookie: test_cookie=CheckForPermission; expires=Fri, 29-Nov-2024 05:24:59 GMT; path=/; domain=.doubleclick.net; Secure; SameSite=none
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

[["soundcloud.com",null,"m.soundcloud.com",null,null,["115535218"]],[],[],null,null,[["115535218",
[["liveintent.indexexchange.com",null,1],["openx.net",null,1],["uidapi.com",null,1],["id5-sync.com",nu
...[SNIP]...
```

12.6. https://securepubads.g.doubleclick.net/tag/js/gpt.js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://securepubads.g.doubleclick.net**
Path:	**/tag/js/gpt.js**

Request

```
GET /tag/js/gpt.js HTTP/1.1
Host: securepubads.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
Accept: */*
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

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 05:09:35 GMT
Expires: Fri, 29 Nov 2024 05:09:35 GMT
Cache-Control: private, max-age=900, stale-while-revalidate=3600
Content-Type: text/javascript; charset=UTF-8
Etag: 779 / 20056 / m202411180101 / config-hash: 2173145291705866055
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Server: cafe
Content-Length: 109511
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

(function(sttc){var window=this;if(window.googletag&&googletag.evalScripts)
{googletag.evalScripts();}if(window.googletag&&googletag._loaded_)return;var n,aa=function(a){var b=0;return function(){retur
...[SNIP]...
```

---

13. Email addresses disclosed

There are 2 instances of this issue:

- https://m.sndcdn.com/_next/static/chunks/c32e057f4d02dbc1f5b44cd40b5e7d23fc6e81ec.58b72375c75190232ffd.js
- https://securepubads.g.doubleclick.net/pagead/managed/js/gpt/m202411180101/pubads_impl.js

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

13.1. https://m.sndcdn.com/_next/static/chunks/c32e057f4d02dbc1f5b44cd40b5e7d23fc6e81ec.58b72375c75190232ffd.js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://m.sndcdn.com**
Path:	**/_next/static/chunks/c32e057f4d02dbc1f5b44cd40b5e7d23fc6e81ec.58b72375c75190232ffd.js**

Issue detail

The following email addresses were disclosed in the response:

- fedor@indutny.com
- git@github.com

Request

```
GET /_next/static/chunks/c32e057f4d02dbc1f5b44cd40b5e7d23fc6e81ec.58b72375c75190232ffd.js HTTP/2
Host: m.sndcdn.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: */*
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://m.soundcloud.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
Content-Type: application/javascript; charset=utf-8
Date: Tue, 26 Nov 2024 11:27:06 GMT
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET
Access-Control-Max-Age: 3000
Last-Modified: Tue, 26 Nov 2024 10:54:42 GMT
Server: AmazonS3
X-Amz-Server-Side-Encryption: AES256
Cache-Control: public, max-age=31536000, immutable
X-Amz-Version-Id: 9bLtsW_FsetQe_f8CGy6WNvPdCo2P6jF
Etag: W/"348280e51d141867500040cf98cad5e4"
Vary: accept-encoding
X-Cache: Hit from cloudfront
Via: 1.1 a1ba4b0527e41da66664ba375de24b7c.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C1
X-Amz-Cf-Id: mT52HoAa-BYWMdlPAAmOSr_HcR0XNstLyYCZNbDf83Tjx6zCD6z5dg==
Age: 236549

(window.webpackJsonp_N_E=window.webpackJsonp_N_E||[]).push([[6],{"+0t7":function(t,e,r){"use strict";r.d(e,"a",(function()
{return h})),r.d(e,"b",(function(){return d})),r.d(e,"e",(function(){return p}
...[SNIP]...
<fedor@indutny.com>
...[SNIP]...
```

13.2. https://securepubads.g.doubleclick.net/pagead/managed/js/gpt/m202411180101/pubads_impl.js

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://securepubads.g.doubleclick.net**
Path:	**/pagead/managed/js/gpt/m202411180101/pubads_impl.js**

Issue detail

The following email address was disclosed in the response:

- robert@broofa.com

Request

```
GET /pagead/managed/js/gpt/m202411180101/pubads_impl.js HTTP/2
Host: securepubads.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
Accept: */*
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://m.soundcloud.com/
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
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Server: cafe
Content-Length: 503686
X-Xss-Protection: 0
Date: Thu, 28 Nov 2024 05:32:56 GMT
Expires: Fri, 28 Nov 2025 05:32:56 GMT
Cache-Control: public, immutable, max-age=31536000
Age: 85000
Etag: 1421939719645060458
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 Google LLC
SPDX-License-Identifier: Apache-2.0
*/
/*


Copyright (c) 2015
...[SNIP]...
NY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
*/
/*

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 ba,da,ja,xa,Aa,Da,Ja,La,Sa,Ua,Va,Wa,Xa,$a,bb,eb,ib,kb,mb,pb,ob,qb,rb,sb,tb,xb,yb,Bb,Db,Fb,Hb,Jb,Kb,Mb,Nb,Ob,P
...[SNIP]...
```

14. Cacheable HTTPS response

There are 12 instances of this issue:

- https://api-mobi.soundcloud.com/me
- https://app-measurement.com/config/app/1:414843287017:android:9d526f6607903f60
- https://app-measurement.com/config/app/1:551011954849:android:c927b6ed30ba0123
- https://cdn.cookielaw.org/consent/7e62c772-c97a-4d95-8d0a-f99bbeadcf61/7e62c772-c97a-4d95-8d0a-f99bbeadcf61.json
- https://emmxuq-cdn-settings.appsflyersdk.com/android/v1/b8f2b4cfb63d3a01ab23168079a65fe4e1df1116866bdd83993e9516912b05a4/settings
- https://emmxuq-dlsdk.appsflyersdk.com/v1.0/android/com.twelve_steps.twelve_steps
- https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location
- https://gmscompliance-pa.googleapis.com/google.internal.gmscore.gmscompliance.v1.GmsCompliance/GetEnforcement
- https://growth-pa.googleapis.com/google.internal.identity.growth.v1.GrowthApiService/GetPromos
- https://securepubads.g.doubleclick.net/pagead/ppub_config
- https://securitydomain-pa.googleapis.com/google.internal.identity.securitydomain.v1.SecurityDomainService/GetSecurityDomain
- https://securitydomain-pa.googleapis.com/google.internal.identity.securitydomain.v1.SecurityDomainService/JoinSecurityDomain

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

14.1. https://api-mobi.soundcloud.com/me

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://api-mobi.soundcloud.com**
Path:	**/me**

Request

```
POST /me?client_id=KKzJxmw11tYpCs6T24P4uUYhqmjalG6M&stage= HTTP/1.1
Host: api-mobi.soundcloud.com
Content-Length: 2321
X-Datadome-Clientid: .keep
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: text/plain;charset=UTF-8
Accept: */*
Origin: https://m.soundcloud.com
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://m.soundcloud.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive

{"events":[{"event":"pageview","version":"v1.27.27","payload":
{"level":"tracks:main","chapter":"","page_name":"tracks:main","page_urn":"soundcloud:tracks:1610873220","referrer_properties
":{"utm_campai
...[SNIP]...
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Content-Length: 0
Connection: keep-alive
date: Fri, 29 Nov 2024 05:10:14 GMT
vary: Origin
x-robots-tag: noindex
referrer-policy: no-referrer
x-frame-options: DENY
access-control-max-age: 1728000
x-content-type-options: nosniff
access-control-allow-origin: https://m.soundcloud.com
access-control-allow-headers: Authorization, Content-Type, Device-Locale, X-CSRF-Token, X-Checkout-Token, X-Client-Id, X-
Datadome-ClientId, X-Payments-Id, X-Payments-Token, X-Request-Id
access-control-allow-methods: DELETE, GET, PATCH, POST, PUT
access-control-expose-headers: Date, X-DD-B, X-Set-Cookie
access-control-allow-credentials: true
strict-transport-security: max-age=63072000
server: am/2
X-Cache: Miss from cloudfront
Via: 1.1 612d3e065148a94cbbe94139733f662e.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: QfhXqAw6rJrX_0aww2xI1qc7KKe3L4QdFPdORsfIrmqY-iWAinpQfw==
```

14.2. https://app-measurement.com/config/app/1:414843287017:android:9d526f6607903f60

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app-measurement.com**
Path:	**/config/app/1:414843287017:android:9d526f6607903f60**

Request

```
GET /config/app/1:414843287017:android:9d526f6607903f60?gmp_version=244534&runtime_version=0&platform=android
HTTP/2
Host: app-measurement.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
Etag: 17195220862225793570
Content-Type: application/x-protobuf
Cross-Origin-Resource-Policy: cross-origin
Content-Security-Policy-Report-Only: script-src 'none'; form-action 'none'; frame-src 'none'; report-uri
https://csp.withgoogle.com/csp/scaffolding/ascgcycc:941:0
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=coop_reporting
Report-To: {"group":"coop_reporting","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-
to/scaffolding/ascgcycc:941:0"}],}
Date: Fri, 29 Nov 2024 05:05:37 GMT
Server: Google Tag Manager
Content-Length: 51671
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

..........'1:414843287017:android:9d526f6607903f60.."%
.measurement.audience.max_count..400"4
-measurement.upload.max_public_user_properties..100"5
-measurement.upload.max_event_name_cardinality..2000
...[SNIP]...
```

14.3. https://app-measurement.com/config/app/1:551011954849:android:c927b6ed30ba0123

Summary

Severity:	**Information**

Confidence: **Certain**

Host: **https://app-measurement.com**

Path: **/config/app/1:551011954849:android:c927b6ed30ba0123**

Request

```
GET /config/app/1:551011954849:android:c927b6ed30ba0123?gmp_version=244534&runtime_version=0&platform=android
HTTP/2
Host: app-measurement.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
Etag: 16786314539300445072
Content-Type: application/x-protobuf
Cross-Origin-Resource-Policy: cross-origin
Content-Security-Policy-Report-Only: script-src 'none'; form-action 'none'; frame-src 'none'; report-uri
https://csp.withgoogle.com/csp/scaffolding/ascgcycc:941:0
Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to=coop_reporting
Report-To: {"group":"coop_reporting","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-
to/scaffolding/ascgcycc:941:0"}],}
Date: Fri, 29 Nov 2024 05:05:27 GMT
Server: Google Tag Manager
Content-Length: 28576
X-Xss-Protection: 0
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

..........'1:551011954849:android:c927b6ed30ba0123.."%
.measurement.audience.max_count..400"4
-measurement.upload.max_public_user_properties..100"5
-measurement.upload.max_event_name_cardinality..2000
...[SNIP]...
```

14.4. https://cdn.cookielaw.org/consent/7e62c772-c97a-4d95-8d0a-f99bbeadcf61/7e62c772-c97a-4d95-8d0a-f99bbeadcf61.json

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://cdn.cookielaw.org**

Path: **/consent/7e62c772-c97a-4d95-8d0a-f99bbeadcf61/7e62c772-c97a-4d95-8d0a-f99bbeadcf61.json**

Request

```
GET /consent/7e62c772-c97a-4d95-8d0a-f99bbeadcf61/7e62c772-c97a-4d95-8d0a-f99bbeadcf61.json HTTP/2
Host: cdn.cookielaw.org
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: */*
Origin: https://m.soundcloud.com
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 05:09:59 GMT
Content-Type: application/json
Content-Length: 6394
Cf-Ray: 8ea016b78d43a304-YUL
Cf-Cache-Status: HIT
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Age: 63008
Cache-Control: public, max-age=86400
Etag: 0x8DCE39CC2310AC9
Expires: Sat, 30 Nov 2024 05:09:59 GMT
Last-Modified: Thu, 03 Oct 2024 11:15:59 GMT
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Vary: Accept-Encoding
Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding
Content-Md5: 05wx44g5Q4oceqOS+jtcRQ==
Cross-Origin-Resource-Policy: cross-origin
X-Content-Type-Options: nosniff
X-Ms-Blob-Type: BlockBlob
X-Ms-Lease-Status: unlocked
X-Ms-Request-Id: 28df8bb9-f01e-00d5-122f-30db57000000
X-Ms-Version: 2009-09-19
Cross-Origin-Resource-Policy: cross-origin
Server: cloudflare

{"CookieSPAEnabled":true,"CookieSameSiteNoneEnabled":true,"CookieV2CSPEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":false,"ScriptType":"PRODUCTION"
...[SNIP]...
```

14.5. https://emmxuq-cdn-settings.appsflyersdk.com/android/v1/b8f2b4cfb63d3a01ab23168079a65fe4e1df1116866bdd83993e9516912b05a4/settings

Summary

Severity:	**Information**
Confidence:	**Certain**

Host: **https://emmxuq-cdn-settings.appsflyersdk.com**

Path: **/android/v1/b8f2b4cfb63d3a01ab23168079a65fe4e1df1116866bdd83993e9516912b05a4/settings**

Request

```
GET /android/v1/b8f2b4cfb63d3a01ab23168079a65fe4e1df1116866bdd83993e9516912b05a4/settings HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; sdk_gphone_x86 Build/RSR1.201013.001)
Host: emmxuq-cdn-settings.appsflyersdk.com
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 200 OK
Content-Type: application/json
Content-Length: 45
Server: awselb/2.0
Date: Thu, 19 Sep 2024 09:51:46 GMT
X-Amz-Meta-Af-Auth-V1: d509a205680c
Via: 1.1 ac1cb1fdb7cf3984f94f9f190169eb3a.cloudfront.net (CloudFront)
Age: 6117231
X-Af-Date: 1732856738
X-Cache: Hit from cloudfront
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: 5QlZxlvoFJo7vVmaSgfuro5xxH0vC2y32SvWtXus1j8irdHK0SmMOg==

{"features":{},"ver":"default.v1.1637149529"}
```

14.6. https://emmxuq-dlsdk.appsflyersdk.com/v1.0/android/com.twelve_steps.twelve_steps

Summary

Severity: **Information**

Confidence: **Certain**

Host: **https://emmxuq-dlsdk.appsflyersdk.com**

Path: **/v1.0/android/com.twelve_steps.twelve_steps**

Request

```
POST /v1.0/android/com.twelve_steps.twelve_steps?
af_sig=c75a71df74d88abaa516b61cc7493a74dd9855a1635936361e0962c84c2b0533&sdk_version=6.13 HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; sdk_gphone_x86 Build/RSR1.201013.001)
Host: emmxuq-dlsdk.appsflyersdk.com
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
Content-Length: 246

{"os":"11","gaid":{"type":"unhashed","value":"f20fbe71-dba0-4c12-8b2e-6cbbc3d4cdfe"},"is_first":false,"lang":"en-
```

```
US","type":"sdk_gphone_x86","request_id":"1732856734123-8428588531524320033","timestamp
...[SNIP]...
```

Response

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Content-Length: 32
Date: Fri, 29 Nov 2024 05:05:37 GMT
Server: http-kit
X-Cache: Miss from cloudfront
Via: 1.1 18b0fca4845f3542d7f0566683e26626.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C2
X-Amz-Cf-Id: F3IYEvVglweSKyYckNj3FoxqIS-SOA7OM8i2A1Ftm2baUrQ_bwZubg==

{"found":false,"click_event":{}}
```

14.7. https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://geolocation.onetrust.com**
Path:	**/cookieconsentpub/v1/geo/location**

Request

```
GET /cookieconsentpub/v1/geo/location HTTP/1.1
Host: geolocation.onetrust.com
Accept: application/json
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
Origin: https://m.soundcloud.com
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://m.soundcloud.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

Response

```
HTTP/2 200 OK
Date: Fri, 29 Nov 2024 05:10:14 GMT
Content-Type: application/json
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Content-Type
Access-Control-Allow-Methods: GET, OPTIONS
Vary: Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

```
Server: cloudflare
Cf-Ray: 8ea017155f9c33f5-YUL

{"country":"CA","state":"QC","stateName":"Quebec","continent":"NA"}
```

14.8. 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: 59494090u
Content-Length: 8253

... 8

.........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 05:05:27 GMT
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Grpc-Status: 0
Endpoint-Load-Metrics-Bin: MURd1dnKUTJASQ5iDO0oStQ/
Grpc-Server-Stats-Bin: AAD1JSoCAAAAAA
Pc-High-Bwd-Bin: S2dJWUNn

....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]...
```

14.9. https://growth-pa.googleapis.com/google.internal.identity.growth.v1.GrowthApiService/GetPromos

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://growth-pa.googleapis.com**
Path:	**/google.internal.identity.growth.v1.GrowthApiService/GetPromos**

Request

```
POST /google.internal.identity.growth.v1.GrowthApiService/GetPromos HTTP/1.1
Host: growth-pa.googleapis.com:443
User-Agent: grpc-java-okhttp/1.31.0-SNAPSHOT
Content-Type: application/grpc
Te: trailers
X-Goog-Api-Key: AIzaSyBXuZXPItcw7joqQCtuR9_yQhXffU_khD4
X-Android-Cert: 38918A453D07199354F8B19AF05EC6562CED5788
X-Android-Package: com.google.android.apps.docs
Grpc-Accept-Encoding: gzip
Authorization: Bearer ya29.m.CoYCAQ1IaZgYeMIbcBW-Dov-DtKaSlh7-
hJqct3LMzL_T9VFZXyng9JyBC2crUHEL3ETPwy1XnRus6YTwcIqzQbkK8HDwxHeg9cg2AF6e3TIOHD3MwVRsjuxINACp3KH
QXYgpxy8fYaOVTBA3tz0a00RILhGZQGgT2tjj5Xmq9fuUdx7LxHLF08DgbY9HbWMtP_yQFk4Y9jBof0loKbdNKCbeoNxawVNa
qd9kPQKZybWHO2NibfsiVd2NLCNARz1ICXADhVL-
Eb08uYNsE1zT3lSLbWJyGNyrJgZQqmrqZRke5lvVxjY6gGajMqdQoCe8eo6fgooQaKI-
1y2Xf02VUtMtlWNSsjkPRIJCAESAxDMHBgAGiBEKikild-WL0U22BAec1xh9smiNFIBa7WoIn-
cfze0vCICCAEqK2FDZ1ILQVJrU0FSSVNGUUhHWDJNaUZXWkUyWDR0TVZjdWY0REVEVTdVR2c
Grpc-Timeout: 17391800u
Content-Length: 136
Connection: keep-alive

.....
  .C.........9.    202220370".com.google.android.apps.docs*.2.20.222.03.70.8..en-US..".30:)
.google..RSR1.201013.001..sdk_gphone_x86".
```

Response

```
HTTP/2 200 OK
Content-Disposition: attachment
Content-Type: application/grpc
Date: Fri, 29 Nov 2024 05:05:27 GMT
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Grpc-Status: 0
Content-Disposition: attachment

.....
```

14.10. https://securepubads.g.doubleclick.net/pagead/ppub_config

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://securepubads.g.doubleclick.net**
Path:	**/pagead/ppub_config**

Request

```
GET /pagead/ppub_config?ippd=m.soundcloud.com HTTP/2
Host: securepubads.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
Accept: */*
Origin: https://m.soundcloud.com
X-Requested-With: com.twelve_steps.twelve_steps
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://m.soundcloud.com/
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
Access-Control-Allow-Origin: *
Date: Fri, 29 Nov 2024 05:09:59 GMT
Expires: Fri, 29 Nov 2024 05:09:59 GMT
Cache-Control: private, max-age=3600, stale-while-revalidate=3600
Content-Type: application/json; charset=UTF-8
X-Content-Type-Options: nosniff
Content-Disposition: attachment; filename="f.txt"
Server: cafe
Content-Length: 2466
X-Xss-Protection: 0
Set-Cookie: test_cookie=CheckForPermission; expires=Fri, 29-Nov-2024 05:24:59 GMT; path=/; domain=.doubleclick.net; Secure; SameSite=none
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

[["soundcloud.com",null,"m.soundcloud.com",null,null,["115535218"]],[],[],null,null,[["115535218",
[["liveintent.indexexchange.com",null,1],["openx.net",null,1],["uidapi.com",null,1],["id5-sync.com",nu
...[SNIP]...
```

14.11. https://securitydomain-pa.googleapis.com/google.internal.identity.securitydomain.v1.SecurityDomainService/GetSecurityDomain

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://securitydomain-pa.googleapis.com**
Path:	**/google.internal.identity.securitydomain.v1.SecurityDomainService/GetSecurityDomain**

Request

```
POST /google.internal.identity.securitydomain.v1.SecurityDomainService/GetSecurityDomain HTTP/2
Host: securitydomain-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-Api-Key: AIzaSyAP-gfH3qvi6vgHZbSYwQ_XHqV_mXHhzIk
X-Android-Package: com.google.android.gms
X-Android-Cert: 38918A453D07199354F8B19AF05EC6562CED5788
X-Goog-Spatula:
CjYKFmNvbS5nb29nbGUuYW5kcm9pZC5nbXMaHE9KR0tSVDBIR1pOVStMR2E4RjdHVml6dFY0Zz0Y8M6FupvDrb04
Authorization: Bearer
ya29.a0AeDClZB1_7AtuMmWmade3eLCXhf5cl8twjaIG9o8Fa3EK1R6Tis8uWGCCLtherUYaUJokod4HOkbQMsj60sDaDPTv4I
eAgJlaNnrh9yAO0dD178FUp-sc1LQF25Wnt-
zYZNjJZgUgo4oOHz5dEOnDN4jirhA3Wi0ioTC8N9AcYibp2FmE0dTV3kDIhqiEs4iZouoJTgTTuQjm0wuXsMz-
5pVyk6AjEKUpX78NzZLbjWnAqDHG2h90MC3h63tOohjS0AZdRynf7Ri7hB1bjkyXy26_52a5zx9gS6NmvYWDRaNTpEGaGbya
5gFbvNo1VALaP0aCgYKAY8SARISFQHGX2MiR3LgS5F5Mb2AHDK0VSPXZg0330
X-Auth-Time: 1732856880521
Grpc-Accept-Encoding: gzip
Grpc-Timeout: 34904925u
Content-Length: 82

....M
#users/me/securitydomains/chromesync...$0f8cca4c-44b3-4c1d-9d1b-31b2e13fe8e3
```

Response

```
HTTP/2 200 OK
Content-Type: application/grpc
Grpc-Accept-Encoding: identity, deflate, gzip
Content-Disposition: attachment
Date: Fri, 29 Nov 2024 05:08:30 GMT
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Grpc-Status: 0
Endpoint-Load-Metrics-Bin: MfEil2Ey03NAOWKU9yH//yRASU/gzxI7j9Q/
Grpc-Server-Stats-Bin: AADQ3WkCAAAAAA
Pc-High-Bwd-Bin: S2dJWUFn

....5
#users/me/securitydomains/chromesync..."...........V
```

14.12. https://securitydomain-pa.googleapis.com/google.internal.identity.securitydomain.v1.SecurityDomainService/JoinSecurityDomain

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://securitydomain-pa.googleapis.com**
Path:	**/google.internal.identity.securitydomain.v1.SecurityDomainService/JoinSecurityDomain**

Request

```
POST /google.internal.identity.securitydomain.v1.SecurityDomainService/JoinSecurityDomain HTTP/2
Host: securitydomain-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-Api-Key: AIzaSyAP-gfH3qvi6vgHZbSYwQ_XHqV_mXHhzIk
X-Android-Package: com.google.android.gms
X-Android-Cert: 38918A453D07199354F8B19AF05EC6562CED5788
X-Goog-Spatula:
CjYKFmNvbS5nb29nbGUuYW5kcm9pZC5nbXMaHE9KR0tSVDBIR1pOVStMR2E4RjdHVml6dFY0Zz0Y8M6FupvDrb04
Authorization: Bearer
ya29.a0AeDClZB1_7AtuMmWmade3eLCXhf5cl8twjaIG9o8Fa3EK1R6Tis8uWGCCLtherUYaUJokod4HOkbQMsj60sDaDPTv4I
eAgJIaNnrh9yAO0dD178FUp-sc1LQF25Wnt-
zYZNjJZgUgo4oOHz5dEOnDN4jirhA3Wi0ioTC8N9AcYibp2FmE0dTV3kDIhqiEs4iZouoJTgTTuQjm0wuXsMz-
5pVyk6AjEKUpX78NzZLbjWnAqDHG2h90MC3h63tOohjS0AZdRynf7Ri7hB1bjkyXy26_52a5zx9gS6NmvYWDRaNTpEGaGbya
5gFbvNo1VALaP0aCgYKAY8SARISFQHGX2MiR3LgS5F5Mb2AHDK0VSPXZg0330
X-Auth-Time: 1732856862604
Grpc-Accept-Encoding: gzip
Grpc-Timeout: 34934338u
Content-Length: 416

.....
%
#users/me/securitydomains/chromesync...
husers/me/members/BCtqB8vJCdCu5XL1FEDQXL2_alU0av4MjVFDrz7tXPDe8mujd0xZ-
OSc7Ui0PF2KKOGIOq_IK7iL2PhiQ3ZQ5oE.A.+j...    ...r..@.\..jU4j...QC.>.\...k.wLY....H.
...[SNIP]...
```

Response

```
HTTP/2 200 OK
Content-Type: application/grpc
Grpc-Accept-Encoding: identity, deflate, gzip
Content-Length: 0
Date: Fri, 29 Nov 2024 05:08:00 GMT
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Grpc-Status: 6
Grpc-Message: Requested entity already exists
Endpoint-Load-Metrics-Bin: MSRHOuHHnHNAOeVuvVTHzCVASWFnfvkVN9E/
Grpc-Server-Stats-Bin: AABxLJMFAAAAAA
Pc-High-Bwd-Bin: S2dJWUJR
```

Google.internal.identity.securitydomain.v1.joinsecuritydomainerrordetail-Bin:
CjcKNQojdXNlcnMvbWUvc2VjdXJpdHlkb21haW5zL2Nocm9tZXN5bmMQhwEiCwjc+P65BhCI+bBW
Grpc-Status-Details-Bin:
CAYSH1JlcXVlc3RlZCBlbnRpdHkgYWxyZWFkeSBleGlzdHMamQEKXHR5cGUuZ29vZ2xlYXBpcy5jb20vZ29vZ2xlLmludGVyb
mFsLmlkZW50aXR5LnNlY3VyaXR5ZG9tYWluLnYxLkpvaW5TZWN1cml0eURvbWFpbkVycm9yRGV0YWlsEjkKNwo1CiN1c2V
ycy9tZS9zZWN1cml0eWRvbWFpbnMvY2hyb21lc3luYxCHASILCNz4/rkGEIj5sFY

15. Base64-encoded data in parameter

Summary

Severity:	**Information**
Confidence:	**Firm**
Host:	**https://api.mixpanel.com**
Path:	**/track/**

Issue detail

The following parameter appears to contain Base64-encoded data:

- **data = [{"event":"$ae_first_open","properties":{"mp_lib":"flutter","$lib_version":"2.3.2","$os":"Android","$os_version":"11","$manufacturer":"Google","$brand":"google","$model":"sdk_gphone_x86","$screen_dpi":420,"$screen_height":1794,"$screen_width":1080,"$app_version":"1.1.7","$app_version_string":"1.1.7","$app_release":"196","$app_build_number":"196","$has_nfc":false,"$has_telephone":true,"$carrier":"Android","$wifi":true,"$bluetooth_version":"ble","token":"c8a613beaa196e54eef479be8b7dc0d1","time":1732856278877,"distinct_id":"$device:f8fd5280-9d08-4ba3-b219-116f9d8d19d5","$had_persisted_distinct_id":false,"$device_id":"f8fd5280-9d08-4ba3-b219-116f9d8d19d5"},"$mp_metadata":{"$mp_event_id":"f48896d49b678d9f","$mp_session_id":"1b687ff16919fc1a","$mp_session_seq_id":0,"$mp_session_start_sec":1732856278}},{"event":"Initial App Launch","properties":{"mp_lib":"flutter","$lib_version":"2.3.2","$os":"Android","$os_version":"11","$manufacturer":"Google","$brand":"google","$model":"sdk_gphone_x86","$screen_dpi":420,"$screen_height":1794,"$screen_width":1080,"$app_version":"1.1.7","$app_version_string":"1.1.7","$app_release":"196","$app_build_number":"196","$has_nfc":false,"$has_telephone":true,"$carrier":"Android","$wifi":true,"$bluetooth_version":"ble","token":"c8a613beaa196e54eef479be8b7dc0d1","time":1732856281694,"distinct_id":"$device:f8fd5280-9d08-4ba3-b219-116f9d8d19d5","$had_persisted_distinct_id":false,"$device_id":"f8fd5280-9d08-4ba3-b219-116f9d8d19d5"},"$mp_metadata":{"$mp_event_id":"693650c14dddc601","$mp_session_id":"1b687ff16919fc1a","$mp_session_seq_id":1,"$mp_session_start_sec":1732856278}},{"event":"Onboard_Experience","properties":{"mp_lib":"flutter","$lib_version":"2.3.2","$os":"Android","$os_version":"11","$manufacturer":"Google","$brand":"google","$model":"sdk_gphone_x86","$screen_dpi":420,"$screen_height":1794,"$screen_width":1080,"$app_version":"1.1.7","$app_version_string":"1.1.7","$app_release":"196","$app_build_number":"196","$has_nfc":false,"$has_telephone":true,"$carrier":"Android","$wifi":true,"$bluetooth_version":"ble","token":"c8a613beaa196e54eef479be8b7dc0d1","time":1732856283236,"distinct_id":"$device:f8fd5280-9d08-4ba3-b219-116f9d8d19d5","$had_persisted_distinct_id":false,"$device_id":"f8fd5280-9d08-4ba3-b219-116f9d8d19d5","Page":"Welcome Page"},"$mp_metadata":{"$mp_event_id":"1d2582170f4b7aa4","$mp_session_id":"1b687ff16919fc1a","$mp_session_seq_id":2,"$mp_session_start_sec":1732856278}},{"event":"Onboard_Experience","properties":{"mp_lib":"flutter","$lib_version":"2.3.2","$os":"Android","$os_version":"11","$manufacturer":"Google","$brand":"google","$model":"sdk_gphone_x86","$screen_dpi":420,"$screen_height":1794,"$screen_width":1080,"$app_version":"1.1.7","$app_version_string":"1.1.7","$app_release":"196","$app_build_number":"196","$has_nfc":false,"$has_telephone":true,"$carrier":"Android","$wifi":true,"$bluetooth_version":"ble","token":"c8a613beaa196e54eef479be8b7dc0d1","time":1732856409918,"distinct_id":"$device:f8fd5280-9d08-4ba3-b219-116f9d8d19d5","$had_persisted_distinct_id":false,"$device_id":"f8fd5280-9d08-4ba3-b219-116f9d8d19d5","Page":"Welcome Page"},"$mp_metadata":{"$mp_event_id":"cfb88e68738fdea5","$mp_session_id":"4ce06f3d5584a30b","$mp_session_seq_id":0,"$mp_ses**

```
sion_start_sec":1732856407}},{"event":"Onboard_Experience","properties":
{"mp_lib":"flutter","$lib_version":"2.3.2","$os":"Android","$os_version":"11","$manufacturer":"Google","$brand"
:"google","$model":"sdk_gphone_x86","$screen_dpi":420,"$screen_height":1794,"$screen_width":1080,"$app_v
ersion":"1.1.7","$app_version_string":"1.1.7","$app_release":"196","$app_build_number":"196","$has_nfc":false,
"$has_telephone":true,"$carrier":"Android","$wifi":true,"$bluetooth_version":"ble","token":"c8a613beaa196e54e
ef479be8b7dc0d1","time":1732856416637,"distinct_id":"$device:f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","$had_persisted_distinct_id":false,"$device_id":"f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","ActionType":"Start your journey"},"$mp_metadata":
{"$mp_event_id":"5e30b404b3b8c1e4","$mp_session_id":"4ce06f3d5584a30b","$mp_session_seq_id":1,"$mp_se
ssion_start_sec":1732856407}},{"event":"Onboard_Experience","properties":
{"mp_lib":"flutter","$lib_version":"2.3.2","$os":"Android","$os_version":"11","$manufacturer":"Google","$brand"
:"google","$model":"sdk_gphone_x86","$screen_dpi":420,"$screen_height":1794,"$screen_width":1080,"$app_v
ersion":"1.1.7","$app_version_string":"1.1.7","$app_release":"196","$app_build_number":"196","$has_nfc":false,
"$has_telephone":true,"$carrier":"Android","$wifi":true,"$bluetooth_version":"ble","token":"c8a613beaa196e54e
ef479be8b7dc0d1","time":1732856416641,"distinct_id":"$device:f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","$had_persisted_distinct_id":false,"$device_id":"f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","Page":"Question Page"},"$mp_metadata":
{"$mp_event_id":"f9cff7c48b637df","$mp_session_id":"4ce06f3d5584a30b","$mp_session_seq_id":2,"$mp_sessi
on_start_sec":1732856407}},{"event":"Onboard_Experience","properties":
{"mp_lib":"flutter","$lib_version":"2.3.2","$os":"Android","$os_version":"11","$manufacturer":"Google","$brand"
:"google","$model":"sdk_gphone_x86","$screen_dpi":420,"$screen_height":1794,"$screen_width":1080,"$app_v
ersion":"1.1.7","$app_version_string":"1.1.7","$app_release":"196","$app_build_number":"196","$has_nfc":false,
"$has_telephone":true,"$carrier":"Android","$wifi":true,"$bluetooth_version":"ble","token":"c8a613beaa196e54e
ef479be8b7dc0d1","time":1732856425073,"distinct_id":"$device:f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","$had_persisted_distinct_id":false,"$device_id":"f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","Page":"Assist Type Page"},"$mp_metadata":
{"$mp_event_id":"f073dce06ad6d4c3","$mp_session_id":"4ce06f3d5584a30b","$mp_session_seq_id":3,"$mp_se
ssion_start_sec":1732856407}},{"event":"Onboard_Experience","properties":
{"mp_lib":"flutter","$lib_version":"2.3.2","$os":"Android","$os_version":"11","$manufacturer":"Google","$brand"
:"google","$model":"sdk_gphone_x86","$screen_dpi":420,"$screen_height":1794,"$screen_width":1080,"$app_v
ersion":"1.1.7","$app_version_string":"1.1.7","$app_release":"196","$app_build_number":"196","$has_nfc":false,
"$has_telephone":true,"$carrier":"Android","$wifi":true,"$bluetooth_version":"ble","token":"c8a613beaa196e54e
ef479be8b7dc0d1","time":1732856445063,"distinct_id":"$device:f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","$had_persisted_distinct_id":false,"$device_id":"f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","Page":"Assist Selection Page"},"$mp_metadata":
{"$mp_event_id":"3d7bbb95a4fc2175","$mp_session_id":"4ce06f3d5584a30b","$mp_session_seq_id":4,"$mp_se
ssion_start_sec":1732856407}},{"event":"Onboard_Experience","properties":
{"mp_lib":"flutter","$lib_version":"2.3.2","$os":"Android","$os_version":"11","$manufacturer":"Google","$brand"
:"google","$model":"sdk_gphone_x86","$screen_dpi":420,"$screen_height":1794,"$screen_width":1080,"$app_v
ersion":"1.1.7","$app_version_string":"1.1.7","$app_release":"196","$app_build_number":"196","$has_nfc":false,
"$has_telephone":true,"$carrier":"Android","$wifi":true,"$bluetooth_version":"ble","token":"c8a613beaa196e54e
ef479be8b7dc0d1","time":1732856450691,"distinct_id":"$device:f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","$had_persisted_distinct_id":false,"$device_id":"f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","Page":"Intro Page"},"$mp_metadata":
{"$mp_event_id":"8f02b5dfb9684d6e","$mp_session_id":"4ce06f3d5584a30b","$mp_session_seq_id":5,"$mp_se
ssion_start_sec":1732856407}},{"event":"Onboard_Experience","properties":
{"mp_lib":"flutter","$lib_version":"2.3.2","$os":"Android","$os_version":"11","$manufacturer":"Google","$brand"
:"google","$model":"sdk_gphone_x86","$screen_dpi":420,"$screen_height":1794,"$screen_width":1080,"$app_v
ersion":"1.1.7","$app_version_string":"1.1.7","$app_release":"196","$app_build_number":"196","$has_nfc":false,
"$has_telephone":true,"$carrier":"Android","$wifi":true,"$bluetooth_version":"ble","token":"c8a613beaa196e54e
ef479be8b7dc0d1","time":1732856463593,"distinct_id":"$device:f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","$had_persisted_distinct_id":false,"$device_id":"f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","Page":"Widget Tour Page"},"$mp_metadata":
{"$mp_event_id":"498dca97563b57f8","$mp_session_id":"4ce06f3d5584a30b","$mp_session_seq_id":6,"$mp_se
ssion_start_sec":1732856407}},{"event":"Onboard_Experience","properties":
{"mp_lib":"flutter","$lib_version":"2.3.2","$os":"Android","$os_version":"11","$manufacturer":"Google","$brand"
:"google","$model":"sdk_gphone_x86","$screen_dpi":420,"$screen_height":1794,"$screen_width":1080,"$app_v
ersion":"1.1.7","$app_version_string":"1.1.7","$app_release":"196","$app_build_number":"196","$has_nfc":false,
"$has_telephone":true,"$carrier":"Android","$wifi":true,"$bluetooth_version":"ble","token":"c8a613beaa196e54e
ef479be8b7dc0d1","time":1732856464820,"distinct_id":"$device:f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","$had_persisted_distinct_id":false,"$device_id":"f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","Page":"Step Bar Tour Page"},"$mp_metadata":
{"$mp_event_id":"b5ec4b6a440cabfa","$mp_session_id":"4ce06f3d5584a30b","$mp_session_seq_id":7,"$mp_se
ssion_start_sec":1732856407}},{"event":"Onboard_Experience","properties":
{"mp_lib":"flutter","$lib_version":"2.3.2","$os":"Android","$os_version":"11","$manufacturer":"Google","$brand"
:"google","$model":"sdk_gphone_x86","$screen_dpi":420,"$screen_height":1794,"$screen_width":1080,"$app_v
```

**ersion":"1.1.7","$app_version_string":"1.1.7","$app_release":"196","$app_build_number":"196","$has_nfc":false,
"$has_telephone":true,"$carrier":"Android","$wifi":true,"$bluetooth_version":"ble","token":"c8a613beaa196e54e
ef479be8b7dc0d1","time":1732856465718,"distinct_id":"$device:f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","$had_persisted_distinct_id":false,"$device_id":"f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","Page":"SpotCheck Tour Page"},"$mp_metadata":
{"$mp_event_id":"b2ae00a0a0ddf3b8","$mp_session_id":"4ce06f3d5584a30b","$mp_session_seq_id":8,"$mp_se
ssion_start_sec":1732856407}},{"event":"Onboard_Experience","properties":
{"mp_lib":"flutter","$lib_version":"2.3.2","$os":"Android","$os_version":"11","$manufacturer":"Google","$brand"
:"google","$model":"sdk_gphone_x86","$screen_dpi":420,"$screen_height":1794,"$screen_width":1080,"$app_v
ersion":"1.1.7","$app_version_string":"1.1.7","$app_release":"196","$app_build_number":"196","$has_nfc":false,
"$has_telephone":true,"$carrier":"Android","$wifi":true,"$bluetooth_version":"ble","token":"c8a613beaa196e54e
ef479be8b7dc0d1","time":1732856466552,"distinct_id":"$device:f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","$had_persisted_distinct_id":false,"$device_id":"f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","Page":"Quotes and Videos Tour Page"},"$mp_metadata":
{"$mp_event_id":"a1cf3bd088f92202","$mp_session_id":"4ce06f3d5584a30b","$mp_session_seq_id":9,"$mp_ses
sion_start_sec":1732856407}},{"event":"Onboard_Experience","properties":
{"mp_lib":"flutter","$lib_version":"2.3.2","$os":"Android","$os_version":"11","$manufacturer":"Google","$brand"
:"google","$model":"sdk_gphone_x86","$screen_dpi":420,"$screen_height":1794,"$screen_width":1080,"$app_v
ersion":"1.1.7","$app_version_string":"1.1.7","$app_release":"196","$app_build_number":"196","$has_nfc":false,
"$has_telephone":true,"$carrier":"Android","$wifi":true,"$bluetooth_version":"ble","token":"c8a613beaa196e54e
ef479be8b7dc0d1","time":1732856467429,"distinct_id":"$device:f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","$had_persisted_distinct_id":false,"$device_id":"f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","Page":"Kai Tour Page"},"$mp_metadata":
{"$mp_event_id":"4a48c9188ba7be7","$mp_session_id":"4ce06f3d5584a30b","$mp_session_seq_id":10,"$mp_se
ssion_start_sec":1732856407}},{"event":"Onboard_Experience","properties":
{"mp_lib":"flutter","$lib_version":"2.3.2","$os":"Android","$os_version":"11","$manufacturer":"Google","$brand"
:"google","$model":"sdk_gphone_x86","$screen_dpi":420,"$screen_height":1794,"$screen_width":1080,"$app_v
ersion":"1.1.7","$app_version_string":"1.1.7","$app_release":"196","$app_build_number":"196","$has_nfc":false,
"$has_telephone":true,"$carrier":"Android","$wifi":true,"$bluetooth_version":"ble","token":"c8a613beaa196e54e
ef479be8b7dc0d1","time":1732856468197,"distinct_id":"$device:f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","$had_persisted_distinct_id":false,"$device_id":"f8fd5280-9d08-4ba3-b219-
116f9d8d19d5","Page":"Resources Tour Page"},"$mp_metadata":
{"$mp_event_id":"f49820029f3c80df","$mp_session_id":"4ce06f3d5584a30b","$mp_session_seq_id":11,"$mp_se
ssion_start_sec":1732856407}}]**

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 /track/?ip=1 HTTP/1.1
Content-Length: 16671
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; sdk_gphone_x86 Build/RSR1.201013.001)
Host: api.mixpanel.com
Connection: keep-alive
Accept-Encoding: gzip, deflate, br

data=W3siZXZlbnQiOiIkYWVfZmlyc3Rfb3BlbiIsInByb3BlcnRpZXMiOnsibXBfbGliIjoiZmx1dHRlciIsIiRsaWJfdmVyc2lvbiI6IjIuMy
4yIiwiJG9zIjoiQW5kcm9pZCIsIiRvc192ZXJzaW9uIjoiMTEiLCIkbWFudWZhY3R1cmVyIjoiR29vZ2xlIiwiJGJyYW5kIjoiZ29vZ2xlIi
wiJG1vZGVsIjoic2RrX2dwaG9uZV94ODYiLCIkc2NyZWVuX2RwaSI6NDIwLCIkc2NyZWVuX2hlaWdodCI6MTc5NCwiJHNjcmVl
bl93aWR0aCI6MTA4MCwiJGFwcF92ZXJzaW9uIjoiMS4xLjciLCIkYXBwX3ZlcnNpb25fc3RyaW5nIjoiMS4xLjciLCIkYXBwX3Jlb
GVhc2UiOiIxOTYiLCIkYXBwX2J1aWxkX251bWJlciI6IjE5NiIsIiRoYXNfbmZjIjpmYWxzZSwiJGhhc190ZWxlcGhvbmUiOnRydW
```

```
UsIiRjYXJyaWVyIjoiQW5kcm9pZCIsIiR3aWZpIjp0cnVlLCIkYmx1ZXRvb3RoX3ZlcnNpb24iOiJibGUiLCJ0b2tlbiI6ImM4YTYxM2
JlYWExOTZlNTRlZWY0NzliZThiN2RjMGQxIiwidGltZSI6MTczMjg1NjI3ODg3NywiZGlzdGluY3RfaWQiOiIkZGV2aWNlOmY4Zm
Q1MjgwLTlkMDgtNGJhMy1iMjE5LTExNmY5ZDhkMTlkNSIsIiRoYWRfcGVyc2lzdGVkX2Rpc3RpbmN0X2lkIjpmYWxzZSwiJGRl
dmljZV9pZCI6ImY4ZmQ1MjgwLTlkMDgtNGJhMy1iMjE5LTExNmY5ZDhkMTlkNSJ9LCIkbXBfbWV0YWRhdGEiOnsiJG1wX2V2
ZW50X2lkIjoiZjQ4ODk2ZDQ5YjY3OGQ5ZiIsIiRtcF9zZXNzaW9uX2lkIjoiMWI2ODdmZjE2OTE5ZmMxYSIsIiRtcF9zZXNzaW9u
X3NlcV9pZCI6MCwiJG1wX3Nlc3Npb25fc3RhcnRfc2VjIjoxNzMyODU2Mjc4fX0seyJldmVudCI6IkluaXRpYWwgQXBwIExhdW5j
aCIsInByb3BlcnRpZXMiOnsibXBfbGliIjoiZmx1dHRlciIsIiRsaWJfdmVyc2lvbiI6IjIuMy4yIiwiJG9zIjoiQW5kcm9pZCIsIiRvc192ZXJ
zaW9uIjoiMTEiLCIkbWFudWZhY3R1cmVyIjoiR29vZ2xlIiwiJGJyYW5kIjoiZ29vZ2xlIiwiJG1vZGVsIjoic2RrX2dwaG9uZV94ODYi
LCIkc2NyZWVuX2RwaSI6NDIwLCIkc2NyZWVuX2hlaWdodCI6MTc5NCwiJHNjcmVlbl93aWR0aCI6MTA4MCwiJGFwcF92ZXJz
aW9uIjoiMS4xLjciLCIkYXBwX3ZlcnNpb25fc3RyaW5nIjoiMS4xLjciLCIkYXBwX3JlbGVhc2UiOiIxOTYiLCIkYXBwX2J1aWxkX25
1bWJlciI6IjE5NiIsIiRoYXNfbmZjIjpmYWxzZSwiJGhhc190ZWxlcGhvbmUiOnRydWUsIiRjYXJyaWVyIjoiQW5kcm9pZCIsIiR3aW
ZpIjp0cnVlLCIkYmx1ZXRvb3RoX3ZlcnNpb24iOiJibGUiLCJ0b2tlbiI6ImM4YTYxM2JlYWExOTZlNTRlZWY0NzliZThiN2RjMGQx
IiwidGltZSI6MTczMjg1NjI4MTY5NCwiZGlzdGluY3RfaWQiOiIkZGV2aWNlOmY4ZmQ1MjgwLTlkMDgtNGJhMy1iMjE5LTExNmY
5ZDhkMTlkNSIsIiRoYWRfcGVyc2lzdGVkX2Rpc3RpbmN0X2lkIjpmYWxzZSwiJGRldmljZV9pZCI6ImY4ZmQ1MjgwLTlkMDgtN
GJhMy1iMjE5LTExNmY5ZDhkMTlkNSJ9LCIkbXBfbWV0YWRhdGEiOnsiJG1wX2V2ZW50X2lk
```

...[SNIP]...

Response

```
HTTP/2 200 OK
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: X-Requested-With, Content-Type
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: X-MP-CE-Backoff
Access-Control-Max-Age: 1728000
Cache-Control: no-cache, no-store
Content-Type: application/json
Strict-Transport-Security: max-age=604800; includeSubDomains
Date: Fri, 29 Nov 2024 05:01:33 GMT
Content-Length: 1
Via: 1.1 google
Alt-Svc: clear

1
```

16. Content type is not specified

There are 2 instances of this issue:

- https://emmxuq-conversions.appsflyersdk.com/api/v6.13/androidevent
- https://emmxuq-launches.appsflyersdk.com/api/v6.13/androidevent

Issue description

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)

16.1. https://emmxuq-conversions.appsflyersdk.com/api/v6.13/androidevent

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://emmxuq-conversions.appsflyersdk.com**
Path:	**/api/v6.13/androidevent**

Request

```
POST /api/v6.13/androidevent?app_id=com.twelve_steps.twelve_steps&buildnumber=6.13.0 HTTP/1.1
Content-Type: application/octet-stream
Content-Length: 3304
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; sdk_gphone_x86 Build/RSR1.201013.001)
Host: emmxuq-conversions.appsflyersdk.com
Connection: keep-alive
Accept-Encoding: gzip, deflate, br

..T2l..&m.g...k.5m..nWY.Y.z,.;)2.....mY.m....hK.Z_...M.9Q8z."c..X...4.....j....."...1
  .n!..l#].....&t..R..X.7.a.....a....To.......s2F.9..W...o....E.8...O-.E...I...'.+....n.p~%u..aS.P.X....4..?YW.7.
...[SNIP]...
```

Response

```
HTTP/2 403 Forbidden
Content-Length: 9
Date: Fri, 29 Nov 2024 05:05:45 GMT
X-Cache: Error from cloudfront
Via: 1.1 1a0361f1d6eeb33d623d41bfabfa3e8e.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YUL62-C1
X-Amz-Cf-Id: ckZh1SeVFDRik3lmAmZ92bNg6T6wKYOOlHTaqA64rAmjzLfZ5qqklg==

forbidden
```

16.2. https://emmxuq-launches.appsflyersdk.com/api/v6.13/androidevent

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://emmxuq-launches.appsflyersdk.com**
Path:	**/api/v6.13/androidevent**

Request

```
POST /api/v6.13/androidevent?app_id=com.twelve_steps.twelve_steps&buildnumber=6.13.0 HTTP/1.1
Content-Type: application/octet-stream
Content-Length: 3064
User-Agent: Dalvik/2.1.0 (Linux; U; Android 11; sdk_gphone_x86 Build/RSR1.201013.001)
Host: emmxuq-launches.appsflyersdk.com
Connection: keep-alive
Accept-Encoding: gzip, deflate, br

O...;V......O..+.N.(./~....?....r|.....b..WU........;Ib..&......|..0%..r......O.......C.....RBP........
[}.....t/.qD.kY.o+Z&....Al...e......]w{..5.h8.........06.&2$.......{..(......u...........K  .n...L
...[SNIP]...
```

Response

```
HTTP/2 403 Forbidden
Content-Length: 9
Date: Fri, 29 Nov 2024 05:09:29 GMT
X-Cache: Error from cloudfront
Via: 1.1 ede5c8e7b29cc9290d2f384042d78428.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: YTO50-P3
X-Amz-Cf-Id: d5HP1bF9Igg2GvsBPgAiWWO-qo9cozPwi0TxmYiuX4ashHYj6b-QNQ==

forbidden
```

Report generated by Burp Suite web vulnerability scanner v2024.9.5, at Fri Nov 29 00:13:30 EST 2024.