



Application	JIRA Plug-in	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Assessment Date	12/11/2023	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	Report Date	12/19/2023

THIS REPORT IS DELIVERED TO THE VENDOR TO ASSIST WITH VULNERABILITY REMEDIATION ACTIVITIES. THIS REPORT DOES NOT CARRY AN ENDORSEMENT FROM THE SOFTWARE SECURITY GROUP.

This report is for GitKraken internal use only and its content cannot be shared or distributed in any form with a third party without prior written consent of KPMG.

[Redacted content]

Instance 1: (Low)

Screenshots:

Host Method URL Params
9866 https://gji-app-us.gforjradcloud.com GET /ui/issue-panel.html?isAdmin=false&isManager=false&hasDevTools=true&issueKey=PTP122023-2&projectKey=PTP122023&projectId=10004&dm_e=https%3A%2F%2Fus-nexus.atlassian.net&dm_c=channel-com.xipin...

Request Response
Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=UTF-8
3 Content-Length: 2306
4 Connection: close
5 Cache-Control: no-cache
6 Cache-Control: no-store
7 Content-Security-Policy: default-src 'self'; img-src 'self' data: https; script-src 'self' 'nonce-bbb_bp_initialize_theming' https://connect-odn.atl-paas.net/all.js
  https://jsd-widget.atlassian.com/assets/embed.js https://jsd-widget.atlassian.com/assets/iframe.js ; style-src 'self' 'unsafe-inline'; connect-src 'self' https://kgqjcxcl8419.statuspage.io
  https://6420435.ingest.sentry.io https://jsd-widget.atlassian.com/api/embeddable/ https://api-private.atlassian.com/gasv3/api/v1/batch; frame-src https://fast.wistia.net
  https://bigtrasshand.atlassian.net;
8 Date: Wed, 13 Dec 2023 07:11:02 GMT
9 Referrer-Policy: origin
10 Server: Git Integration for Jira Cloud
11 Strict-Transport-Security: max-age=31536000; includeSubDomains
12 X-XSS-Protection: 1; mode=block
13 X-Cache: Miss from cloudfront
14 Via: 1.1 3203c4b5504fa019a752072f0419ef6a.cloudfront.net (CloudFront)
15 X-Amz-CF-Pop: IAD12-P3
16 X-Amz-CF-Id: qP2T2FHHdyrk2LYeRB6Pee5nXCYOQo2LRABuikYok505Jjtv-VUw==
17
18 <!doctype html>
19 <html lang="en">
20 <head>
21 <meta name="color-scheme" content="dark light">
22 <script defer src="/ui/manifest.68cae59622042446393a.js">
23 </script>
24 <script defer src="/ui/init.2e781e361420ab6d2679.js">
25 </script>
26 <script defer src="/ui/issuePanel.70cb5790c712057d0b5a.js">
27 </script>
28 <link href="/ui/styles/out.686545d3925d0665afaf.css" rel="stylesheet">
29 <meta name="sentry-dsn" content="https://3024538c220443988f61dd1003e927420e420435.ingest.sentry.io/5338610">
30 <meta name="sentry-environment" content="prod-us">
31 </head>
32 <body style="overflow: hidden">
33 <section id="content" class="ac-content">
34 <div id="bbb-gp-spinner" style="
35 height: 100vh;
36 display: flex;
37 align-items: center;">
38 <style>
39 @keyframes spinnerRotateAnimation{
40
```



[Redacted]

[Redacted]

Remediation

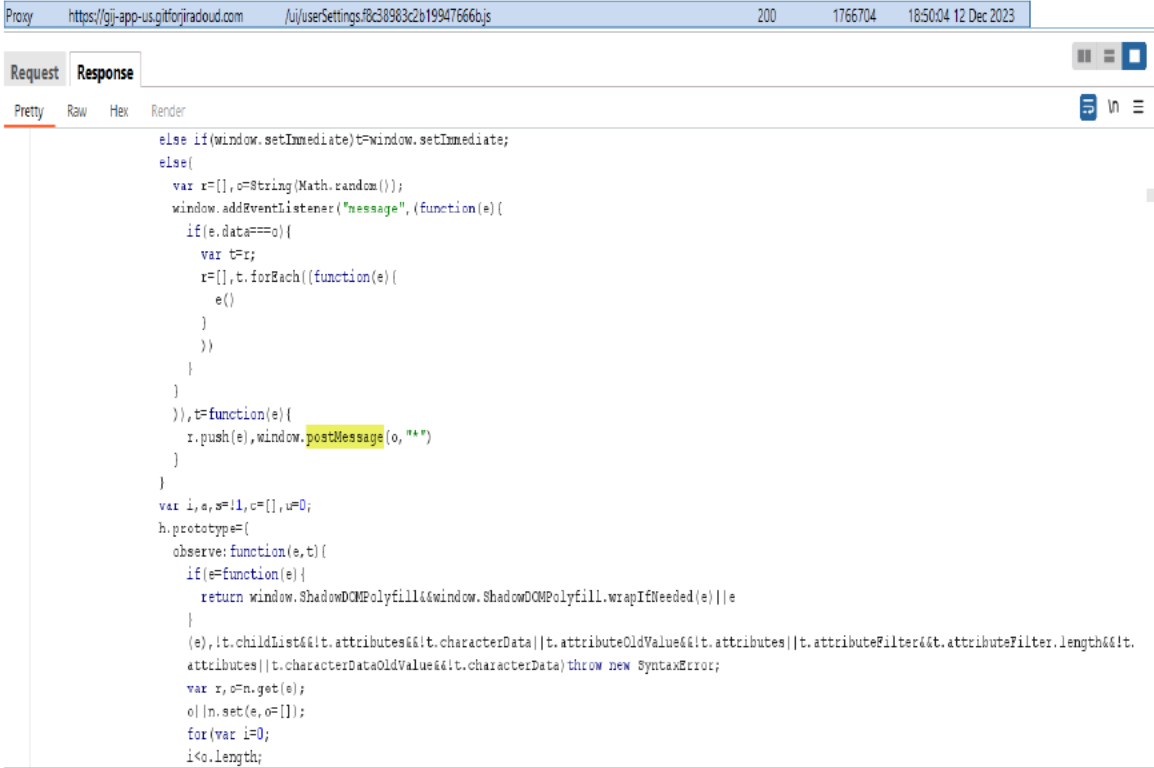
Enable X-FRAME-OPTIONS protection. X-Frame-Options Header Types
There are three possible values for the X-Frame-Options headers:
DENY, which prevents any domain from framing the content.
SAMEORIGIN, which only allows the current site to frame the content.
ALLOW-FROM uri, which permits the specified 'uri' to frame this page (NOTE:
Not all browsers support this option).

**(Closing/Down
grading)
Justification**

[Redacted]

Vulnerability	8. Overly Permissive postMessage() Policy		Status	Open
Risk Rating	Low	Vulnerability Owner	Application	
Issue Description:	<p>The <code>postMessage()</code> function is one of the features of HTML5 that allows a window to send messages to another open window. The typical syntax of <code>postMessage</code> is <code>window.postMessage(message, targetOrigin, [transfer])</code>. The use of this function was observed in one of the client-side scripts. The "message" parameter contains the information to be shared and "targetOrigin" indicates the origin of the destination window. The use of wildcard (*) allows the message to be shared with any window. If a malicious user injects a new window into the javascript's execution context, then the new window will now be able to receive any information that is shared using the vulnerable <code>postMessage</code> construct.</p>			
URL	https://gij-app-us.gitforjiracloud.com/ui/userSettings.f8c38983c2b19947666b.js			

Screenshots:



Remediation	All data that is shared between windows must have explicit origins to avoid eavesdropping. It is recommended to avoid using "*" for the "targetOrigin"
--------------------	--

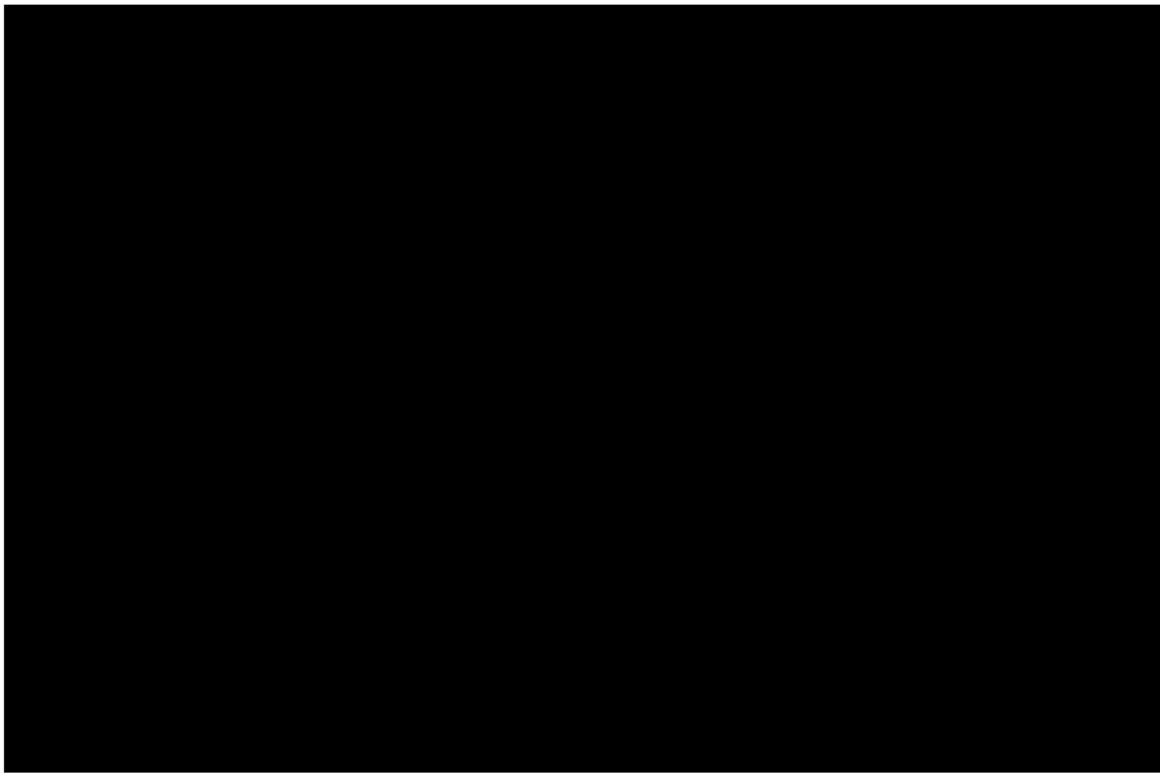
	in order to prevent a broadcast of the information. It is also important to validate any message that is received from another window.
(Closing/Down grading) Justification	

E3MDI0NzM0OTUsImIhdCI6MTcwMjQ3MjU5NX0.RxFeW-iJbr6Oj1uTjMs-
aPqCJYEyJaoevUFkV1rxXEs

[REDACTED]

[REDACTED]

[REDACTED]



Instance 2: (Low)

Screenshots:

The screenshot shows a web browser's developer tools interface. The top bar indicates a GET request to `https://jira-ppp-us.gtforyradoud.com`. The response is HTML, with the following headers:

- 1 HTTP/1.1 200 OK
- 2 Content-Type: text/html; charset=UTF-8
- 3 Content-Length: 2306
- 4 Connection: close
- 5 Cache-Control: no-cache
- 6 Cache-Control: no-store
- 7 Content-Security-Policy: default-src 'self'; img-src 'self' data: https; script-src 'self' 'nonce-bbb_bp_initialize_theming' https://connect-cdn.atl-pssw.net/all.js https://jira-widjet.atlassian.com/assets/embed.js https://jira-widjet.atlassian.com/assets/iframe.js; style-src 'self' 'unsafe-inline'; connect-src 'self' https://kgjcxsl8419.statuspage.io https://o420431.ingest.sentry.io https://jira-widjet.atlassian.com/api/embeddable/ https://api-private.atlassian.com/gasv3/api/v1/batch; frame-src https://fast.wistia.net https://highcontrast.atlassian.net;
- 8 Date: Mon, 10 Dec 2023 08:54:02 GMT
- 9 Referrer-Policy: origin
- 10 Server: Git Integration for Jira Cloud
- 11 Strict-Transport-Security: max-age=31536000; includeSubDomains
- 12 X-Frame-Options: ip mod=block
- 13 X-Cache: Miss from CloudFront
- 14 Via: 1.1 3042b456c0ca8a79JDe6896b8e85e9e.cloudfront.net (CloudFront)
- 15 X-Amz-CF-POP: DAL12-P3
- 16 X-Amz-CF-Id: w8fgik7haq6tweqlf8wvWUXpjz6G9UnlX0cmLl100U0G8a20pww==


The response body starts with `<!doctype html>` and `<html lang="en">`. The `<head>` section includes:

- `<meta name="color-scheme" content="dark light">`
- `<script defer src="/ui/manifest.68cae5622d4294c93a.js">`
- `</script>`
- `<script defer src="/ui/init.2e701e361420ab6d2075.js">`
- `</script>`
- `<script defer src="/ui/issuePanel.70cb579071D057d0b5a.js">`
- `</script>`
- `<link href="/ui/styles/out.f85d4d39254066544f.css" rel="stylesheet">`
- `<meta name="entry-dsn" content="https://3024530e220441908461d1003e927426e404035.ingest.sentry.io/5336610">`
- `<meta name="entry-environment" content="prod-us">`

The `</head>` section ends with `</head>`. The `<body>` section starts with `<body style="overflow: hidden">` and contains a `<section id="content" class="sc-content">` with a `<div id="bbb-gp-spinner" style="height: 100vh; display: flex; align-items: center;">` and `</div>`.

Basic Latin New Tab eicar-standard-anti... Pre-Prod Pen Test R... String Encoder / De... AJAX Security - OW... 2FA/OTP Bypass - H... Exploiting cache de...

CSP Evaluator



CSP Evaluator allows developers and security experts to check if a Content Security Policy (CSP) serves as a strong mitigation against [cross-site scripting attacks](#). It assists with the process of reviewing CSP policies, which is usually a manual task, and helps identify subtle CSP bypasses which undermine the value of a policy. CSP Evaluator checks are based on a [large-scale study](#) and are aimed to help developers to harden their CSP and improve the security of their applications. This tool (also available as a [Chrome extension](#)) is provided only for the convenience of developers and Google provides no guarantees or warranties for this tool.

Content Security Policy

[Sample unsafe policy](#) [Sample safe policy](#)

```
default-src 'self'; img-src 'self' data: https; script-src 'self' 'nonce-bbb_bp_initialize_theming'
https://connect-cdn.atl-paas.net/all.js https://jsd-widget.atlassian.com/assets/embed.js
https://jsd-widget.atlassian.com/assets/iframe.js; style-src 'self' 'unsafe-inline'; connect-src 'self'
https://kgajcvcl8419.statuspage.io https://o420435.ingest.sentry.io https://jsd-widget.atlassian.com/api/embeddable/
https://api-private.atlassian.com/gasv3/api/v1/batch; frame-src https://fast.vistia.net
https://bigbrassband.atlassian.net;
```

CSP Version 3 (nonce based + backward compatibility checks)

CHECK CSP

Evaluated CSP as seen by a browser supporting CSP Version 3 [expand/collapse all](#)

- ✓ default-src
- ✓ img-src
- ✗ script-src
 - Host whitelists can frequently be bypassed. Consider using 'strict-dynamic' in combination with CSP nonces or hashes.
 - Consider adding 'unsafe-inline' (ignored by browsers supporting nonces/hashes) to be backward compatible with older browsers.
- ✓ style-src
- ✓ connect-src
- ✓ frame-src
- ✗ base-uri [missing]
 - Missing base-uri allows the injection of base tags. They can be used to set the base URL for all relative (script) URLs to an attacker controlled domain. Can you set it to 'none' or 'self'?
- ✗ object-src [missing]
 - Can you restrict object-src to 'none'?
- ✗ require-trusted-types-for [missing]
 - Consider requiring Trusted Types for scripts to lock down DOM XSS injection sinks. You can do this by adding 'require-trusted-types-for 'script'' to your policy.

Remediation

Basic CSP policy should be implemented. This policy will only allow resources from the originating domain for all the default level directives and will not allow inline scripts/styles to execute. If your application functions with these restrictions, it drastically reduces your attack surface and will work with most modern browsers. For configuring the CSP, please refer to the below links: - <https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP> <https://csp-evaluator.withgoogle.com/>

(Closing/Down grading) Justification

Vulnerability	14. Using Components with Known Vulnerabilities		Status	Open
Risk Rating	Low	Vulnerability Owner	Application	
Issue Description:	During pen test, it was observed that the application uses older version of the components like jQuery. There are many known exploits for these versions which can affect the application.			
URL	<p><u>Instance 1:</u></p> <p>https://gij-app-us.gitforjiracloud.com/ui/lib/jquery-3.4.1.min.js</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>			
<u>Instance 1: (Low)</u>				
<u>Screenshots:</u>				

Host Method URL
585 https://gij-app-us.gitforjradoud.com GET /ui/lib/jquery-3.4.1.min.js

```
Request Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Content-Type: application/javascript; charset=utf-8
3 Connection: close
4 Vary: Accept-Encoding
5 Cache-Control: max-age=2592000, public
6 Content-Security-Policy: default-src 'self'; img-src 'self' data: https; script-src 'self' 'nonce-bbb_bp_initialize_theming' https://connect-cdn.atl-paas.net/all.js https://jsd-widget.atlassian.com/assets/embed.js https://jsd-widget.atlassian.com/assets/iframe.js; style-src 'self' 'unsafe-inline'; connect-src 'self' https://kgjxcxl8419.statuspage.io https://o420433.lingest.sentry.io https://jsd-widget.atlassian.com/api/embeddable/ https://api-private.atlassian.com/gasv3/api/v1/batch; frame-src https://fast.wistia.net https://bigbrassband.atlassian.net;
7 Date: Mon, 18 Dec 2023 07:44:01 GMT
8 Referer-Policy: origin
9 Server: Git Integration for Java Cloud
10 Strict-Transport-Security: max-age=31536000; includeSubDomains
11 X-SS-Protection: 1; mode=block
12 X-Cache: Miss from cloudfront
13 Via: 1.1 f57a09c5455a80253c61001d750462e6.cloudfront.net (CloudFront)
14 X-Amz-CF-Pop: IAD12-P3
15 X-Amz-CF-Id: H4e617aMc7R8W24du_reFNPHDMuXIXhqoR5XPf1ln55Cqj-iIvoldw==
16 Content-Length: 88145
17
18 /*! jQuery v3.4.1 | (c) JS Foundation and other contributors | jquery.org/license */
19 !function(e,t){
20   "use strict";
21   "object"===typeof module&&"object"===typeof module.exports?module.exports=e.document?t(e,t):function(e){
22     if(!e.document)throw new Error("jQuery requires a window with a document");
23     return t(e)
24   }
25   :t(e)
26 }
27 ("undefined"===typeof window?window:this,function(C,e){
28   "use strict";
29   var t=[],B=C.document,r=Object.getPrototypeOf,s=t.slice,g=t.concat,u=t.push,i=t.indexOf,n=
30   {},oFn.toString,v=n.hasOwnProperty,w=v.toString,l=a.call(Object),y=(
31   ),
32   m=function(e){
33     return"function"===typeof e&&"number"!==typeof e.nodeType
34   },
35   x=function(e){
36     return null!==e&&e===e.window
37   },
38   c={
```

security.snyk.io/package/npm/jquery/3.4.1

Snyk Vulnerability Database · npm · jquery · jquery@3.4.1

jquery@3.4.1 vulnerabilities

JavaScript library for DOM operations

Direct Vulnerabilities
Known vulnerabilities in the jquery package. This does not include vulnerabilities belonging to this package's dependencies.

Automatically find and fix vulnerabilities affecting your projects. Snyk scans for vulnerabilities and provides fixes for free.

[Fix for free](#)

VULNERABILITY	VULNERABLE VERSION
M Cross-site Scripting (XSS)	>=1.5.1 <3.5.0

jquery is a package that makes things like HTML document traversal and manipulation, event handling, animation, and Ajax much simpler with an easy-to-use API that works across a multitude of browsers.

LATEST VERSION
3.7.1

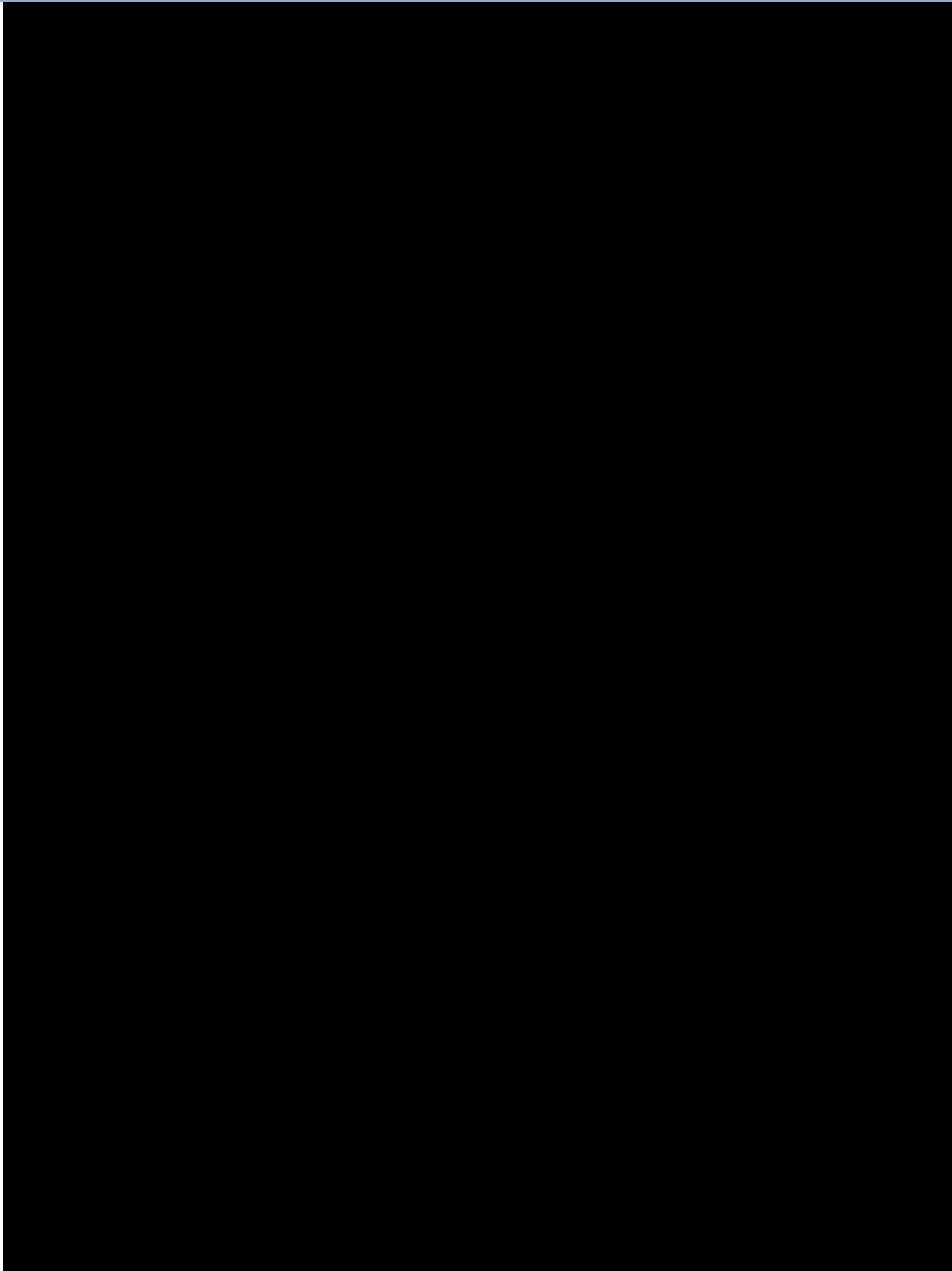
LATEST NON VULNERABLE VERSION
3.7.1

FIRST PUBLISHED
13 years ago

LATEST VERSION PUBLISHED
4 months ago

LICENSES DETECTED
MIT >=1.7.2





Remediation

Upgrade to the latest version.

(Closing/Down grading) Justification	
---	--