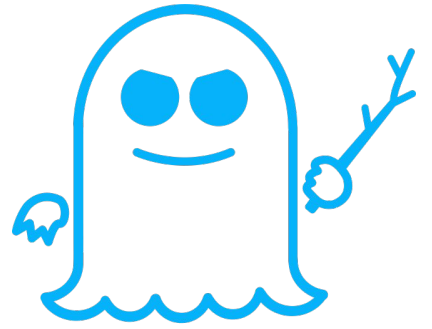


Spectre/Chrome

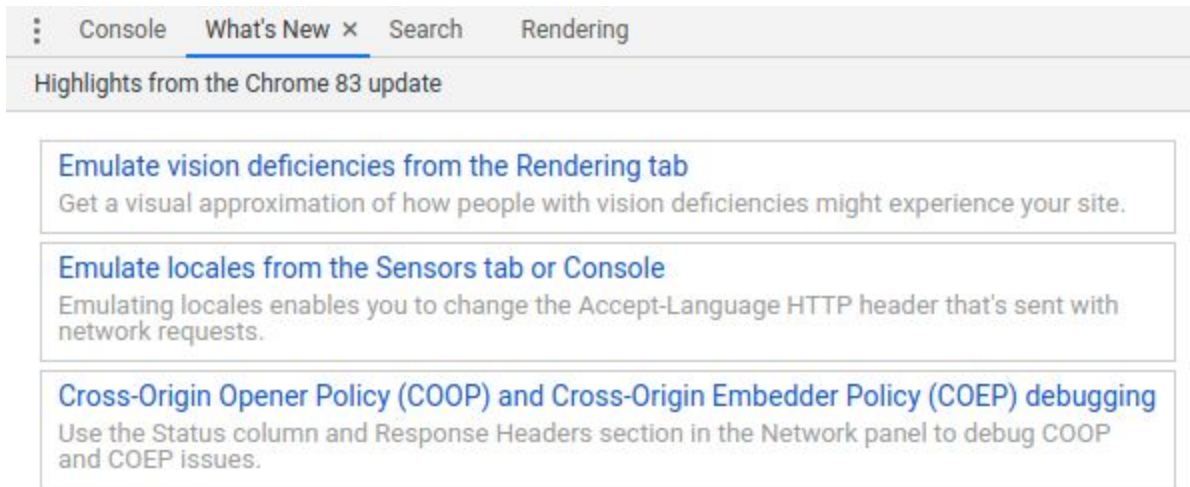
2 ans plus tard...



SPECTRE



What's New in Chrome 83



The image shows a screenshot of the Chrome DevTools interface. At the top, there is a navigation bar with a menu icon, followed by the tabs 'Console', 'What's New' (which is active and underlined), 'Search', and 'Rendering'. Below this is a header for the 'What's New' tab that reads 'Highlights from the Chrome 83 update'. The main content area contains three distinct boxes, each with a blue link and a descriptive paragraph.

⋮ Console **What's New** × Search Rendering

Highlights from the Chrome 83 update

[Emulate vision deficiencies from the Rendering tab](#)
Get a visual approximation of how people with vision deficiencies might experience your site.

[Emulate locales from the Sensors tab or Console](#)
Emulating locales enables you to change the Accept-Language HTTP header that's sent with network requests.

[Cross-Origin Opener Policy \(COOP\) and Cross-Origin Embedder Policy \(COEP\) debugging](#)
Use the Status column and Response Headers section in the Network panel to debug COOP and COEP issues.

Emulate Visual Deficiencies

Achromatique



Who is the OWASP® Foundation?

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

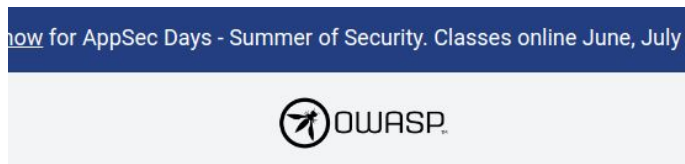


Who is the OWASP® Foundation?

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

No visual deficiency



Who is the OWASP®

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

For nearly two decades, corporate



Who is the O

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

For nearly two decades, corporate

Flou

Daltonien

COOP & COEP debugging

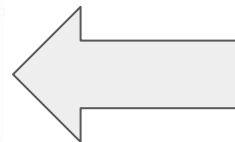
⋮ Console What's New × Search Rendering

Highlights from the Chrome 83 update

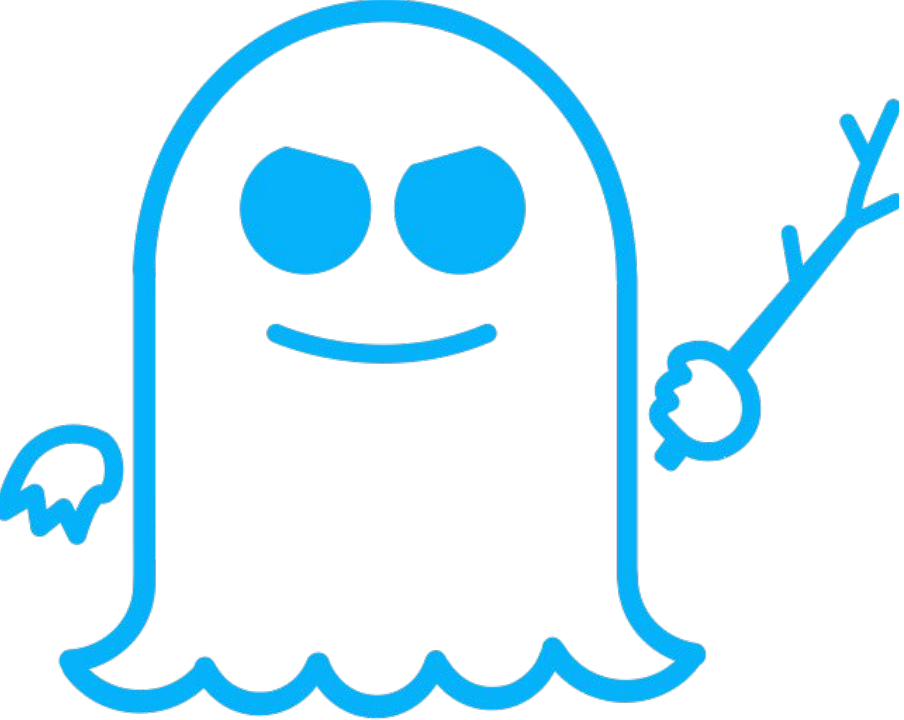
[Emulate vision deficiencies from the Rendering tab](#)
Get a visual approximation of how people with vision deficiencies might experience your site.

[Emulate locales from the Sensors tab or Console](#)
Emulating locales enables you to change the Accept-Language HTTP header that's sent with network requests.

[Cross-Origin Opener Policy \(COOP\) and Cross-Origin Embedder Policy \(COEP\) debugging](#)
Use the Status column and Response Headers section in the Network panel to debug COOP and COEP issues.



Hum...



SPECTRE

Spectre



- Time-based side-channel attack on the CPU.
- Speculative execution from branch misprediction
- Attaquant a besoin
 - D'une horloge de haute précision
 - De pouvoir exécuter du code sur la machine cible



Impact on Chrome

- Un attaquant peut lire la mémoire de Chrome via Javascript
- SharedBufferArray

Chrome

- Micro-code optimisation
- Site Isolation
- CORB
- CORP
- COEP
- COOP

Site Isolation

- Same Origin Policy
- Assigne un processus à chaque site
- Out-Of-Process iframe
- Site \neq Origine
- Chrome
 - SHIFT + ESC
 - <chrome://process-internals/#general>

SharedArrayBuffer

Shared Array Buffer - OTHER

Usage % of all users
Global 33.05%

Type of ArrayBuffer that can be shared across Workers.

Current aligned Usage relative Date relative Apply filters Show all ?

IE	Edge	Firefox	Chrome	Safari	Opera	iOS Safari	Opera Mini	Android Browser	Opera Mobile	Chrome for Android	Firefox for Android	UC Browser for Android	Samsung Internet	QQ Browser	Baic Brow:
	12-15 16-18	2-56 57-73	4-59 60-67		10-46 47-63										
6-10	79-81	74-76	68-81	10.1-13	64-67	10.3-13.3		2.1-4.4.4	12-12.1				4-10.1		
11	83	77	83	13.1	68	13.5	all	81	46	81	68	12.12	11.2	10.4	7.1
		78-79	84-86	TP											

<https://caniuse.com/#feat=sharedarraybuffer>

CORB

Quid si le site Site A contient le code suivant?

```

```

```
<script src="https://SiteB/secrets.json" async />
```

Démo: <https://anforowicz.github.io/xsdb-demo/index.html>

CORB

⚠ Cross-Origin Read Blocking (CORB) blocked cross-origin response http://localhost:8001/secrets.json with MIME type text/plain. See https://www.chromestatus.com/feature/5629709824032768 for more details.	test.html:6
⚠ Cross-Origin Read Blocking (CORB) blocked cross-origin response http://localhost:8001/secrets.data with MIME type text/plain. See https://www.chromestatus.com/feature/5629709824032768 for more details.	test.html:7
⚠ Cross-Origin Read Blocking (CORB) blocked cross-origin response http://localhost:8001/another-secret.data with MIME type application/json. See https://www.chromestatus.com/feature/5629709824032768 for more details.	test.html:9

Mais, le développeur doit ajouter les en-têtes:

- X-Content-Type: nosniff
- Content-Type

Cross-Origin-Resource-Policy

- CORB: automatique... mais bloque seulement si:
 - HTML MIME type - "text/html"
 - XML MIME type - "text/xml", "application/xml", ...
 - JSON MIME type - "text/json", "application/json", ...
- CORP: En-tête pour protéger n'importe quelle ressource
- Cross-Origin-Resource-Policy: same-site | same-origin | cross-origin
 - same-site: seules les requêtes provenant du même site sont possibles
 - same-origin: seules les requêtes provenant de la même origine sont possibles
 - cross-origin: same-site + same-origin

[https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy_\(CORP\)](https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy_(CORP))

Cross-Origin Embedder Policy

- Empêche un site de charger une ressource avec une origine qui ne l'a pas explicitement autorisée via CORS ou CORP
- Empêche aussi le chargement de “workers” ou de “frames” qui ne l'ont pas autorisés via l'en-tête : Cross-Origin-Embedder-Policy: require-corp

NOT-SET cross-origin-resource-policy

To use this resource from a different origin, the server needs to specify a cross-origin resource policy in the response headers:

Cross-Origin-Resource-Policy: same-site — Choose this option if the resource and the document are served from the same site.

Cross-Origin-Resource-Policy: cross-origin — Only choose this option if an arbitrary website including this resource does not impose a security risk.

[→ Learn more](#)

Cross-Origin-Opener-Policy

- Un page/document peut demander un nouveau groupe de contexte de navigation
- Généralement: un groupe de context \Leftrightarrow processus
- COOP: en-tête à ajouter
- Cross-Origin-Opener-Policy: same-origin | same-origin-allow-popups | unsafe-none
- Démo: <https://first-party-test.glitch.me/coop>

Chrome

- Site Isolation + COOP ⇒
Isoler les sites
- CORB + CORP + COEP
⇒ Empêcher le
chargement de ressources
sensibles

