Hedis - Scan sécurité Avril 2025

Fichier à récupérer sur le disque local :
- Stockage_Salariés/Quentin/HEDIS Sécurité/BCE_FR_HEDIS_WAS_REPORT_20250401.html

aednet.fr

Pas de faille de niveau 3

bhe-hedis.fr

Vulnerability - Path Disclosure

Predictable Resource Location Via Forced Browsing (last time detected/tested 28 Mars 2025)

Concerne des fichiers/dossiers trouvés en crawlant le site, c'est "dangereux" que si le lien (disons la page) en question comporte des informations sensibles, pour bhe-hedis, ce n'est pas le cas. Ce qui est affiché est normalement public et/ou souhaité par la société.

Vérifier quand même car il est vrai que pour certaines URL, on peut taper des choses bizarres (qui ne sont pas vraiment des pages réelles) et on est pas renvoyés sur un 404 not found. Je ne sais pas en soit si c'est dangereux, mais autant interdire ce genre de choses dans le doute ?

Par exemple : https://bhe-hedis.fr/actualites-detail/40/includes/

https://bhe-hedis.fr/actualites-detail/51/php/

Vulnerability - Information Disclosure

Clickjacking - Framable page (last time detected/tested 25 Octobre 2024)

Pour bhe-hedis, j'ai vérifié les dates et dans ce qui est noté dans le PDF, pas de nouveau tests depuis la date écrite ci-dessus, donc normalement c'est OK de notre côté (il fallait appliquer une Content Security Policy self-ancestor quelque chose de mémoire en entête HTTP du site/des pages). Je ne sais pas pourquoi les alertes sont toujours notées comme "actives".

Use of JavaScript Library With Known Vulnerability (last time detected/tested 28 Mars 2025)

En effet, Jquery est en version 2.2.4 et apparemment les versions au-dessus de 2.2.2 et en-dessous de 3.0.0 ont beaucoup de failles XSS. Donc il faut patcher.

Pareil pour la seconde librairie concernée, bootstrap JS qui est en version 3.3.7 et il faut au moins la 3.4.1 pour également éviter du XSS.

Reverse Tabnapping (last time detected/tested 28 Mars 2025)

Menace : *Reverse Tabnabbing is an attack where the target page is replaced by phishing site. This is possible when target="_blank" is in use with rel="noopener" or rel="noreferrer", attacker can use JavaScript window.opener and inject malicious domain in it. When user clicks on html link, they will get redirected to phishing or unintentional website.*
WAS detects this vulnerability during crawling and evaluates HTML links embedded in anchor tags.

Impact : *The user may be redirected to an untrusted page that contains undesired content or malicious script code.*

Solution :
1. Use either of these attributes rel="noreferrer" or rel="noopener".
2. Implement Cross Origin Opener Policy header.

En gros, en fouillant le HTML, là où il y a un target=_blank, généralement sur une balise a href/a target, il faut rajouter une balise en plus ou bien (voir si ça fonctionne tout seul) mettre en place une COOP (Cross Origin Opener Policy) qui est une entête HTTP (https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cross-Origin-Opener-Policy)

daugeron.fr

Vulnerability - Path Disclosure

Predictable Resource Location Via Forced Browsing (last time detected/tested 28 Mars 2025)

Pareil que bhe-hedis, ce qui est affiché est normalement public et/ou souhaité par la société.

Vulnerability - Information Disclosure

Pareil que bhe-hedis (mettre à jour jQuery, Bootstrap) et le Reverse Tabnapping (les target=_blank)

fichot-hygiene.fr

Vulnerability - Path Disclosure

Predictable Resource Location Via Forced Browsing (last time detected/tested 28 Mars 2025)

Pareil que daugeron.fr, ce qui est affiché est normalement public et/ou souhaité par la société.

Vulnerability - Information Disclosure

Pareil que daugeron.fr (mettre à jour jQuery, Bootstrap) et le Reverse Tabnapping (les target=_blank)

ica-hygiene.com

Vulnerability - Path Disclosure

Predictable Resource Location Via Forced Browsing (last time detected/tested 28 Mars 2025)

Pareil que fichot-hygiene.fr, ce qui est affiché est normalement public et/ou souhaité par la société.

Vulnerability - Information Disclosure

Pareil que fichot-hygiene.fr (mettre à jour jQuery, Bootstrap) et le Reverse Tabnapping (les target=_blank)

sas-blanc.com

Vulnerability - Path Disclosure

Predictable Resource Location Via Forced Browsing (last time detected/tested 28 Mars 2025)

Pareil que ica-hygiene.com, ce qui est affiché est normalement public et/ou souhaité par la société.

Vulnerability - Information Disclosure

Pareil que ica-hygiene.com (mettre à jour jQuery, Bootstrap) et le Reverse Tabnapping (les target=_blank)

sodiscol.fr

Vulnerability - Path Disclosure

Predictable Resource Location Via Forced Browsing (last time detected/tested 28 Mars 2025)

Pareil que sas-blanc.com, ce qui est affiché est normalement public et/ou souhaité par la société.

Vulnerability - Information Disclosure

Pareil que sas-blanc.com (mettre à jour jQuery, Bootstrap) et le Reverse Tabnapping (les target=_blank)

www.gama29.fr

Pas de faille de niveau 3

www.groupe-hedis.com

Vulnerability - Path Disclosure

Predictable Resource Location Via Forced Browsing (last time detected/tested 28 Mars 2025)

Pareil que sodiscol.com, ce qui est affiché est normalement public et/ou souhaité par la société.

Vulnerability - Information Disclosure

Passive Mixed Content Vulnerability (first time detected 26 Mai 2023, last time detected 28 Mars 2025)

Il semblerait que ça soit dû à la présence d'un lien/d'une image sur la page, appelé(e) en HTTP alors que le site est HTTPS. Il faudrait charger l'image problématique en HTTPS (si elle existe toujours) sinon dans notre cas ici, ça ne semble plus exister du tout donc la retirer.

Par exemple : Sur la page https://www.groupe-hedis.com/nos-actualites/11/ chargée en HTTPS, l'image en question qui pose problème (et qui n'existe plus) est appelée via le lien

http://www.groupe-hedis.com/wp-content/uploads/2018/04/paquerette.png

> Le site n'est plus un Wordpress depuis un moment, donc lien à supprimer ou remplacer par une image "pas d'image" ou "Not found".

Concernant les autres failles de ce site, c'est pareil que sodiscol.com (mettre à jour jQuery, Bootstrap) et le Reverse Tabnapping (les target=_blank)

www.nicolasentretien.fr

Vulnerability - Path Disclosure

Predictable Resource Location Via Forced Browsing (last time detected/tested 28 Mars 2025)

Pareil que groupe-hedis.com, ce qui est affiché est normalement public et/ou souhaité par la société.

Vulnerability - Information Disclosure

Pareil que groupe-hedis.com (mettre à jour jQuery, Bootstrap) et le Reverse Tabnapping (les target=_blank)

www.orru-hedis.fr

Vulnerability - Information Disclosure

Pareil que groupe-hedis.com (mettre à jour jQuery, Bootstrap) et le Reverse Tabnapping (les target=_blank)

www.sopecal-hygiene.com

Vulnerability - Path Disclosure

Predictable Resource Location Via Forced Browsing (last time detected/tested 28 Mars 2025)

Pareil que nicolas-entretien.com, ce qui est affiché est normalement public et/ou souhaité par la société.

Vulnerability - Information Disclosure

Pareil que nicolas-entretien.com (mettre à jour jQuery, Bootstrap) et le Reverse Tabnapping (les target=_blank)

Concernant le fait de mettre à jour jQuery et Boostrap, ça serait logique d'appliquer ça sur les autres sites (pas que ceux d'Hedis) aussi car ils comportent très certainement les mêmes vulnérabilités.

Revision #6
Created 9 April 2025 13:21:56 by Quentin
Updated 10 April 2025 13:14:46 by Quentin