Registre des violations

Violations

Rétention erronée log Caddy

11/10/2023 : Lors de l'audit régulier du système, découverte que Caddy, le serveur web utilisé, ne permet pas de limiter correctement la durée de rétention des logs. Les logs, supposés être conservés pendant 15 jours, conformément à l'arrêt Télé2 de la CJUE, l'ont été en réalité depuis le 15 août 2023 16:49:58. La période concernée correspond à 3101 accès web depuis 289 adresses IPv6 et 591 IPv4 différentes. Tous les accès ne sont pas des personnes concernées au titre du RGPD, la présence de crawler (Fediverse, indexation...) étant notable (70-80%), la distinction précise entre les 2 catégories étant difficile à faire et peu pertinente ici.

Les logs concernés ont été supprimés immédiatement et une migration de l'infrastructure vers Nginx est planifiée avant le 15/10/2023. Le retour à Caddy ne se fera qu'après un correctif permettant de se mettre en conformité.

Les risques pour les droits des personnes concernées étant nuls (correction rapide, pas de perte de confidentialité, aucun usage des données) aucune notification de l'APD n'a été jugée nécessaire ni aucune notification aux personnes concernées.

Non désactivation des logs de debug de dnsdist

06/03/2024 : Dans le cadre d'une mise-à-jour régulière du registre de traitement, un audit des systèmes en place a été conduit pour s'assurer de la cohérence avec les traitements listés. Il a été détecté que le dnsdist déployé en sous-traitance pour relayer le trafic DNS IPv4 vers la machine virtuelle de l'association avait le debug actif, ce qui a conduit à tracer les requêtes effectuées dans les journaux système. Le debug avait été activé le 17/08/2023 pour diagnostiquer un problème de communication DNS, mais n'avait pas été désactivé ensuite.

À la date de la détection du défaut de configuration, 3369 adresses IP, majoritairement des IP sur des plages m2m mais contenant aussi des IP domestiques, étaient encore présentes dans les journaux. Le sous-traitant a aussitôt notifié l'association et procédé à la désactivation du debug.

Les risques pour les droits des personnes concernées étant nuls (pas d'accès à l'information, rétention limitée à 15 jours, IP essentiellement m2m, données non sensibles) et aucun défaut d'intégrité/disponibilité/confidentialité n'ayant été détecté, aucune notification de l'APD n'a été jugée nécessaire ni aucune notification aux personnes concernées.

Mauvaise configuration de la rétention dans journalctl

19/09/2024 : journalctl avait été configuré de manière à ne conserver les logs systèmes que pour 1 mois. Le paramètre utilisé, `MaxFileSec=1month` n'était pas le bon et ne conduisait pas nécessairement à purger les données passées 1 mois et des données personnelles, en particulier des adresses emails liés à la journalisation de opensmtpd étaient présentes 2 mois de trop (période du 21 juin au 21 août). La configuration a été modifiée pour utiliser `MaxRetentionSec=1month` à la place. Les journaux ont été confirmés comme ne démarant plus qu'à partir du 21 août :

```
# journalctl | head -1
août 21 23:36:17
```

Les risques pour les droits des personnes concernées étant nuls (pas d'accès à l'information, rétention limitée à 3 mois, données non sensibles) et aucun défaut d'intégrité/disponibilité/confidentialité n'ayant été détecté, aucune notification de l'APD n'était donc possible.

Activation incontrôlée de la télémétrie Mattermost

10/08/2025 : lors de la mise-à-jour du Mattermost en version 10.10.1, la télémétrie s'est retrouvée activée sans raison.

Elle a été désactivée et les CSP de l'application ont été durcies pour éviter un éventuel problème identique par la suite.

```
more_set_headers "Content-Security-Policy: default-src 'self'; style-src 'self' 'unsafe-inline'; style-src-attr 'unsafe-inline'; script-src 'self'; img-src 'self' data: *;" always;
```

Une déclaration de violation de données a été faite à la CNIL (n° FR2508101800001). Les Personnes Concernées ont été prévenues le jour-même, bien que l’effet sur leurs droits soit négligeable.

Revision #4
Created 2024-08-15 19:45:40 UTC by aeris
Updated 2025-08-10 16:16:16 UTC by aeris