Post-Mortem : Incident 29/05/2026

Résumé de l'incident

Le vendredi 29 mai 2026, entre 11h14 et 11h25 UTC+2 (soit une durée de 11 minutes), une erreur de configuration sur notre réseau de distribution de contenu (CDN) a provoqué la mise en cache involontaire des réponses de nos API.

En conséquence, certains utilisateurs ont pu visualiser à l'écran des informations appartenant à d'autres utilisateurs de leur organisation.

L'incident a été détecté en interne en quelques minutes, la configuration a été corrigée à 11h21, avec un retour à la normale côté serveur dès 11h25. En raison de la nature des données concernées (données à caractère personnel), nous avons immédiatement activé notre cellule de crise, puis, dans un second temps (14h après l'incident) notifié par e-mail individuellement l'ensemble des clients concernés, en communiquant les logs associés permettant à chaque client de réaliser une analyse sur les données concernées.

Un facteur a toutefois pu prolonger les effets de l'incident au-delà de ces 11 minutes : le cache des navigateurs des utilisateurs *(voir la section Impact)*.

Chronologie des événements du 29/05/2026

- **11h14 :** Déploiement par Lucca d'une modification de la configuration de cache sur notre CDN. Cette modification a produit l'effet inverse de celui recherché : au lieu d'empêcher la mise en cache de certaines réponses, elle a activé la mise en cache des réponses d'API.
- **11h15 :** Début effectif de la mise en cache des réponses.
- **11h19 :** Premier signalement et ouverture de l'incident par nos équipes.
- **11h21 :** Identification de la cause, désactivation de la règle et purge du cache.
- **11h22-11h24 :** Déploiement de la configuration corrigée (règle de cache désactivée), et qualification en incident de sécurité : Fin des effets de cache sur notre plateforme.
- **11h27 :** Activation de la cellule de crise.
- **Après-midi :**
    - Correctifs pour forcer le nettoyage des caches au sein des navigateurs.
    - Extraction des logs, évaluation précise des clients impactés.
- **15h25 :** Fin des effets résiduels dans les caches navigateur (sur disque) des utilisateurs finaux.
- **Fin de journée :**

    - Corrélations des logs CDN avec les IP et utilisateurs connectés.
    - Consolidation des descriptions et niveau de criticité des routes.
    - Vérification de l'exactitude des logs.
- **30 mai 00h55 - 01h04 :** Notification individuelle de tous les clients concernés par e-mail incluant les logs détaillés des routes impactées par criticité et des utilisateurs concernés.

Impact

- **Nature de l'exposition :** L'incident était limité à un **affichage non autorisé** de données, en **lecture seule**. **Aucune modification, suppression ou export de données n'était possible.** Un utilisateur ne pouvait pas choisir les informations qu'il voyait : il voyait ce que le cache lui servait, sans pouvoir cibler une personne en particulier.
- **Fonctionnement de l'exposition :** Pour une page donnée, les informations du **premier utilisateur** ayant consulté cette page après l'activation du cache étaient mémorisées, puis **présentées aux utilisateurs suivants** consultant la même page. Le cache de notre CDN étant indexé **par requête et non par utilisateur**, un collaborateur pouvait ainsi voir s'afficher, dans son propre écran, le nom ou des informations d'un **autre collaborateur de son organisation**.
- **Le facteur de prolongation d'impact via le cache des navigateurs :** L'effet principal a duré 11 minutes côté serveur. Seuls les utilisateurs ayant consulté des pages durant cette fenêtre ont été concernés par cette prolongation : les données alors affichées (par exemple le nom apparaissant dans le bandeau de l'application) ont pu rester stockées localement dans le cache de leur navigateur pour une durée pouvant aller jusqu'à 4 heures. Ces effets résiduels ont disparu à 15h25.
- **Données concernées :** Les données exposées présentaient un caractère personnel : informations d'identité (nom, prénom, e-mail) et, selon les écrans consultés, des informations RH plus larges (établissement, compteurs d'absences, contrats). Dans **un nombre plus limité de cas**, des données plus "sensibles" ont pu être affichées (justificatifs d'absence, éléments liés à la paie). Tous les clients concernés ont été contactés et ont reçu une **analyse de logs détaillée et personnalisée**.
- **Périmètre de l'exposition** : Le périmètre s'est limité aux données de l'organisation. Aucune personne extérieure à l'organisation n'a pu accéder aux données.

Cause Racine

La cause principale est une **erreur humaine de configuration du cache** sur notre CDN (CloudFlare). Une modification destinée à empêcher la mise en cache de réponses d'erreur (en 404) a, par un effet de bord, activé la mise en cache des réponses de nos API (l'inverse de l'intention initiale). Cette modification a fait l'objet d'un déploiement préalable en pré-production (et sur un seul domaine) sans permettre de détecter l'erreur.

Deux facteurs organisationnels ont permis à cette erreur d'atteindre la production :

- **Une revue défaillante :** sur un changement pourtant critique, la modification a été validée par une seule personne (autre que celle proposant la modification) avec un niveau de séniorité insuffisant et cette revue n'a pas soulevé d'objection.
- **Une recette inadaptée :** La procédure de test n'a pas été réalisée avec une méthode permettant de détecter un défaut de mise en cache (vérification multi-utilisateur, ou vérification des headers de cache sur les appels d'API).

Notre approche suite à cet incident du 29 mai 2026 vise donc à mettre en place plusieurs niveaux de contrôles indépendants, de sorte qu'aucune erreur isolée ne puisse à nouveau reproduire ce type d'incident.

Actions Correctives et Préventives

Nous vous détaillons ci-dessous notre plan d'action, lequel a été conçu dans l'objectif de multiplier les points de contrôles et de réduction du risque.

Actions déjà réalisées :

1. Renforcement du contrôle des modifications de cache : toute modification de la configuration de cache requiert désormais l'**approbation de 4 personnes nominativement identifiées et qualifiées**, avant toute validation de changement. Plus aucune modification de règle de cache ne peut être validée par une seule personne et sans l'aval de ces 4 relecteurs nominativement identifiés. Cette mesure de protection à court terme permet de verrouiller le risque.

Actions en cours de réalisation :

2. Protection à la source : nous allons ajouter des directives explicites « ne pas mettre en cache » directement sur nos API (via des headers), **côté serveur**. Cette mesure supplémentaire, indépendante du CDN, réduirait fortement le risque de mise en cache des réponses d'API en cas de future erreur de configuration.

3. Recette automatisée : mise en place de tests automatisés échouant si une réponse d'API est mise en cache.
4. Détection automatisée : création d'une alerte déclenchée par tout comportement anormal de mise en cache de nos API, avec déclenchement d'incident automatique.
5. Capacité de révocation des caches navigateur et mobile : pouvoir, en cas d'incident, déconnecter l'ensemble des utilisateurs concernés et purger de manière fiable les caches navigateur et mobile.

6. Déploiement progressif des changements de configuration : mise en place d'un processus de déploiement par lot (avec une granularité plus fine que pré-production / production), afin qu'une modification ne puisse impacter l'ensemble de nos clients simultanément.

Actions à l'étude, ETA début 2027 :

7. Réduction de notre dépendance au cache : nous réévaluons l'intérêt du cache et la solution utilisée pour notre cache CDN afin de déterminer si cet usage peut être réduit, voire totalement supprimé. Le remplacement de notre solution actuelle (Cloudflare) par une solution WAF seule (sans CDN) permettrait de supprimer totalement le risque d'incident de règle de cache.
8. Contacts d'urgence dans l'Espace Client : comme annoncé en 2025, nous poursuivons la fiabilisation des contacts **Sécurité et DPO** de votre organisation, afin de vous joindre **dans les meilleurs délais** en cas d'incident. Nous vous encourageons à vérifier et à tenir à jour ces informations essentielles. Pour ajouter ou mettre à jour ces contacts Sécurité et DPO, consultez notre fiche d'aide disponible ici.

Conclusion

Nous tenons à vous présenter nos plus sincères excuses pour cet incident. Soyez assurés que la sécurité de vos données et votre confiance sont notre priorité.

Ce plan d'action que nous vous partageons vise à réduire au maximum le risque lié à l'usage du mécanisme de cache à court terme et à étudier les évolutions structurelles permettant de le supprimer à moyen terme.

Pour être informé en temps réel de tout incident ou opération de maintenance, nous vous invitons également à vous abonner à notre page Statut : https://status.lucca.fr

Nous restons à votre entière disposition pour toute question, via votre interlocuteur habituel ou nos contacts sécurité et DPO : security@luccasoftware.com et dpo@luccasoftware.com

Cordialement,

Fait à Nantes, le 11/06/2026

Raphaël DUCOM
Chief Information Security Officer