LPS **Presta Software**
Les Logiciels Presta inc.

VITRINE · RAPPORT D'OBSERVATION DE SÉCURITÉ · V0.69

# Rapport d'observation de sécurité : Presta Software Inc.

| | | | |
|---|---|---|---|
| À | Presta Software Inc., propriétaire de prestasoftware.com | | |
| DE | Marco Presta, Presta Software Inc. | DATE | 2026-11-07 |
| OBJET | Vérification en lecture seule de prestasoftware.com le 2026-11-07 à 15 h 46 UTC : 1 de gravité moyenne, 1 de gravité faible, 9 pour information | | |

## CE QUI EST À VOUS, CE QUI EST À VOTRE PLATEFORME

Les 11 points ci-dessous sont à votre charge, ou à celle de la personne qui s'occupe de votre site.

DIFFUSION Pour vous, propriétaire du site, avec votre accord. Ni publié ni communiqué à qui que ce soit d'autre.

## POURQUOI VOUS RECEVEZ CE RAPPORT

Avec votre accord, j'ai vérifié en lecture seule votre site Web public **prestasoftware.com** le 2026-11-07 à 10 h 46, heure de l'Est (relevé technique : horodatage 2026-11-07T15:46:27Z, exécution 2026-11-07). Mon outil a envoyé 7 requêtes en tout, toutes à prestasoftware.com : 6 demandes de page ordinaires, comme celles d'un navigateur, et 1 vérification de la connexion sécurisée. Il a seulement lu ce qui revenait; rien n'a été modifié, mis à l'épreuve ni forcé (détails sous *Comment l'observation a été faite*). Les lignes qui touchent la sécurité sont en annexe (quelques vérifications de conception du site, sans lien avec la sécurité, sont laissées de côté) et les éléments de preuve conservés sont disponibles sur demande. Pour mémoire, votre accord est « consigné le 2026-11-07 : own-site sample for the Vitrine collateral ».

## CE QU'UN INCONNU APPREND SUR VOTRE SITE EN UNE HEURE, SANS Y TOUCHER

Chaque ligne dit ce qui est visible de l'extérieur. Aucune ne dit qu'il est arrivé quoi que ce soit à votre site.

**Qui fait fonctionner ce site, et sur quoi**

- Les noms DNS de votre domaine et le nom de son réseau sont visibles dans les registres publics

**Quels noms existent**

- Des noms vus dans les journaux publics de certificats

**Vos adresses et votre courriel**

- Votre politique DMARC est p=none : les serveurs de réception ne prennent aucune mesure à l'égard du courrier qui échoue

**Ce qui se charge aussi sur vos pages**

- Services tiers observés sur la page d'entrée

## CE QUI COMPTE LE PLUS, PAR ORDRE D'IMPORTANCE

## VOTRE PAGE DE CONFIDENTIALITÉ ET VOS TRACEURS

À partir de la même réponse de la page d'entrée déjà lue plus haut (aucune requête supplémentaire) : signal du lien de confidentialité, groupes de services tiers et noms de témoins placés avant le consentement.

Au Québec, la Loi 25 demande à une entreprise qui recueille des renseignements personnels en ligne de publier une politique de confidentialité claire qui nomme ses témoins et ses tiers.

- **Aucun lien vers la page de confidentialité n'a été détecté sur la page d'entrée** `privacy-link-missing` MOYENNE OBSERVÉ. Nous n'avons trouvé aucun lien vers une page de confidentialité dans votre page d'entrée telle que le serveur l'envoie d'abord (texte ou adresse du lien). Un lien ajouté ensuite par un script n'apparaîtrait pas dans cette analyse. Les visiteurs pourraient ne pas trouver votre politique rapidement. *Que faire :* Ajoutez un lien visible, en en-tête ou en pied de page, vers votre politique de confidentialité à partir de la page d'entrée, dans la langue de la page. *Référence :* bonne pratique. *Observé :* `https://prestasoftware.com: no privacy link (looked for privacy / confidentialité / vie privée / privacidade / renseignements personnels / données personnelles / donnees personnelles / personal information / Loi 25 / Law 25 in anchor text or href)`
- **Services tiers observés sur la page d'entrée** `third-parties-listed` INFORMATION OBSERVÉ. Les services tiers vus sur la page d'entrée sont regroupés ainsi : analytique: aucun; publicité: aucun; gestionnaire d'étiquettes: aucun; contenus intégrés: aucun; clavardage: aucun; autres: static.cloudflareinsights.com. *Que faire :* Utilisez cette liste groupée pour mettre à jour votre politique de confidentialité et votre registre interne des technologies. *Référence :* bonne pratique. *Observé :* `https://prestasoftware.com: analytics: none; ads_pixels: none; tag_managers: none; embeds: none; chat: none; other: static.cloudflareinsights.com`

---

## POUR INFORMATION

- **Aucune ligne CAA n'est publiée pour votre domaine** [caa-missing, information, registre public : lu dans le DNS ou au registre du domaine, jamais sur le site]. Votre domaine **prestasoftware.com** ne publie aucune ligne CAA. Cette ligne peut nommer l'autorité de certification autorisée à émettre des certificats pour votre domaine. *Que faire :* Demandez à la personne qui gère votre DNS et vos certificats d'ajouter une ligne CAA, ou de confirmer pourquoi il n'en faut pas. *Référence :* RFC 8659 (CAA). *Observé :* `prestasoftware.com CAA: no CAA record`
- **La politique de style autorise le style intégré (« unsafe-inline »)** `csp-weak-style` INFORMATION OBSERVÉ. Les règles de style de votre Content-Security-Policy autorisent encore le style intégré (`style-src allows 'unsafe-inline'`). *Que faire :* Privilégiez les feuilles de style externes, ou utilisez des empreintes/nonces pour les blocs de style qui doivent rester. *Référence :* W3C Content Security Policy niveau 3. *Observé :* `https://prestasoftware.com: style-src allows 'unsafe-inline'`
- **Des noms vus dans les journaux publics de certificats** [ct-names-seen, information, registre public : lu dans le DNS ou au registre du domaine, jamais sur le site]. Les journaux publics de certificats listent ces noms sous **prestasoftware.com** : www.prestasoftware.com. Ils ont été lus dans les journaux seulement; aucun de ces noms n'a été contacté. *Que faire :* Confirmez que chaque nom est attendu; si l'un est ancien ou inconnu, revoyez où son certificat est utilisé. *Référence :* journaux publics de certificats (certspotter et crt.sh). *Observé :* `prestasoftware.com CT names: www.prestasoftware.com; these names were not contacted`
- **Les noms DNS de votre domaine et le nom de son réseau sont visibles dans les registres publics** [dns-host-named, information, registre public : lu dans le DNS ou au registre du domaine, jamais sur le site]. Les registres DNS publics de **prestasoftware.com** nomment ces serveurs DNS : beau.ns.cloudflare.com, martha.ns.cloudflare.com. La fiche RDAP publique de la première adresse A pointe vers ce nom de réseau : CLOUDFLARENET. *Que faire :* Gardez cette ligne comme « qui contacter » quand le DNS tombe : ces noms et ce réseau sont votre point de départ. *Référence :* registres DNS et RDAP publics. *Observé :* `prestasoftware.com NS: beau.ns.cloudflare.com, martha.ns.cloudflare.com; who to ask: CLOUDFLARENET`
- **Aucune ligne DS de DNSSEC n'est publiée pour votre domaine** [dnssec-off, information, registre public : lu dans le DNS ou au registre du domaine, jamais sur le site]. Votre domaine **prestasoftware.com** n'a aucune ligne DS dans la zone parente; DNSSEC n'y est donc pas publié. *Que faire :* Demandez à votre fournisseur DNS ou à votre registraire si DNSSEC peut être activé, puis publiez la ligne DS dans la zone parente. *Référence :* RFC 4033-4035 (DNSSEC). *Observé :* `prestasoftware.com DS: no DS record at the parent zone`
- **Aucune ligne DNS MTA-STS n'est publiée pour votre domaine** [mta-sts-missing, information, registre public : lu dans le DNS ou au registre du domaine, jamais sur le site]. Votre domaine **_mta-sts.prestasoftware.com** n'a aucune ligne TXT à _mta-sts._mta-sts.prestasoftware.com; aucune politique MTA-STS n'y est donc annoncée. *Que faire :* Si vous recevez du courriel sur ce domaine, demandez à votre fournisseur de courriel s'il faut publier MTA-STS. *Référence :* RFC 8461 (MTA-STS). *Observé :* `_mta-sts.prestasoftware.com TXT: no TXT record`

- **Aucune ligne DNS TLS-RPT n'est publiée pour votre domaine** [tls-rpt-missing, information, registre public : lu dans le DNS ou au registre du domaine, jamais sur le site]. Votre domaine **_smtp._tls.prestasoftware.com** n'a aucune ligne TXT avec v=TLSRPTv1 à _smtp._tls._smtp._tls.prestasoftware.com; les rapports SMTP TLS n'y sont donc pas configurés. *Que faire :* Demandez à votre fournisseur de courriel s'il faut publier une ligne TLS-RPT et où envoyer les rapports. *Référence :* RFC 8460 (rapports SMTP TLS). *Observé :* `_smtp._tls.prestasoftware.com TXT: no v=TLSRPTv1 record`

## VOTRE COURRIER ET VOTRE DOMAINE

Ces points viennent de registres publics, pas de votre site Web : les réglages de courrier que votre domaine **prestasoftware.com** publie dans le DNS, lus par un résolveur DNS public, et la fiche publique de ce domaine au registre. Aucune de ces lectures n'a atteint votre serveur.

- **Votre politique DMARC est p=none : les serveurs de réception ne prennent aucune mesure à l'égard du courrier qui échoue** [dmarc-none, faible, registre public : lu dans le DNS ou au registre du domaine, jamais sur le site]. Votre ligne DMARC ( `v=DMARC1; p=none; rua=mailto:lps01@prestasoftware.com` ) demande aux serveurs de réception de ne prendre aucune mesure à l'égard du courrier qui échoue aux vérifications; p=none est la première étape habituelle. Les rapports vont à mailto:lps01@prestasoftware.com; le risque est donc visible pour la personne qui les lit. *Que faire :* Lisez les rapports pendant quelques semaines et dressez la liste de chaque service qui envoie vraiment votre courrier, puis faites passer la politique à p=quarantine, et plus tard à p=reject. *Référence :* RFC 7489 (DMARC), section 6.3. *Observé :* `_dmarc.prestasoftware.com TXT: "v=DMARC1; p=none; rua=mailto:lps01@prestasoftware.com"; p=none; reports to mailto:lps01@prestasoftware.com`
- **Votre ligne SPF nomme des services externes qui peuvent envoyer du courrier en votre nom** [spf-names-left-services, information, registre public : lu dans le DNS ou au registre du domaine, jamais sur le site]. La ligne SPF de votre domaine permet à ces services externes d'envoyer du courrier en votre nom : _spf.mx.cloudflare.net. Chacun est une permission accordée à un moment donné; un service que vous n'utilisez plus peut encore envoyer du courrier qui passe pour le vôtre. *Que faire :* Confirmez chaque nom auprès de la personne qui gère votre courriel, et retirez ceux que vous n'utilisez plus; rien ici ne dit qu'un service fait quoi que ce soit de mal. *Référence :* RFC 7208 (SPF), section 5.2. *Observé :* `prestasoftware.com TXT: "v=spf1 include:_spf.mx.cloudflare.net ~all"; names: _spf.mx.cloudflare.net`

## COMMENT L'OBSERVATION A ÉTÉ FAITE

En clair : l'outil a ouvert votre page comme le fait le navigateur d'un visiteur, a regardé quelques fichiers standard, et ne s'est pas connecté, n'a rempli aucun formulaire et n'a rien tenté de forcer. Le relevé, pour la personne qui s'occupe de votre site :

Agent utilisateur (User-Agent) `vitrine-observe/0.1 (Presta Software; passive observation; +https://www.prestasoftware.com/en/vitrine/)` . Vos journaux montrent cette chaîne User-Agent. Par hôte, seulement : l'adresse d'entrée ( `https://prestasoftware.com/` , redirections du serveur suivies, au plus 5 sauts), la forme http:// de cette adresse pour un seul saut, /.well-known/security.txt, /robots.txt, un chemin inexistant choisi exprès, /sitemap.xml, au plus une adresse .map, celle d'un script du site lui-même, et, si l'entrée répond en https://, une négociation TLS limitée à la version 1.2 (plus une limitée à la version 1.3, seulement si la connexion d'entrée n'utilisait pas déjà la 1.3). Au plus 13 contacts par hôte, à au moins 1 s d'intervalle, délai d'attente de 20 s, au plus une nouvelle tentative, arrêt après toute réponse 403 ou 429. Code d'état HTTP au bout de la chaîne d'entrée : 200. Aucun POST, aucun formulaire, aucune connexion à un compte, aucune énumération de chemins, aucune exploitation de faille. La gravité est la cote fixe que l'outil donne à chaque règle, et non une évaluation de votre risque. Lors de cette exécution : 7 contacts en tout, tous avec prestasoftware.com, aucun avec un autre hôte. Pages suivies (0) : none. Les registres publics de votre domaine ont été lus à part, par des services publics (un résolveur DNS, le registre du domaine), jamais sur votre site; ils ne font pas partie de ces contacts.

## CONTEXTE

La référence à côté de chaque point est la norme qu'il cite; la gravité est la cote fixe que l'outil donne à chaque règle, et non une évaluation de votre risque. Rien ici ne constitue un constat de conformité, et c'est votre propre jugement sur votre site qui prime.

## PROCHAINE ÉTAPE

Répondez-moi si vous voulez le relevé conservé pour votre site (la liste des requêtes, avec leurs heures et leurs réponses) ou une deuxième analyse après un changement de votre part (vous m'avez permis de regarder votre site jusqu'au 2026-12-05). Pour

faire revérifier un point, remettez à la personne qui s'occupe de votre site le fichier joint 00-HOW-TO-REPRODUCE-fr.md. Ce rapport n'est pas publié et ne le sera pas; il n'est remis qu'à vous.

## REFAIRE CES VÉRIFICATIONS VOUS-MÊME

Le fichier joint 00-HOW-TO-REPRODUCE-fr.md s'adresse à la personne qui s'occupe de votre site Web, ou à un technicien que vous engagez : il lui permet de refaire ces mêmes vérifications en lecture seule quand elle le veut, et il explique comment lire les résultats. Vous n'avez rien à exécuter vous-même. Il ne lit que ce que tout visiteur peut voir; utilisez-le seulement sur des sites qui vous appartiennent ou que vous avez l'autorisation de vérifier.

## ANNEXE : LIGNES OBSERVÉES POUR CE SITE

| règle | gravité | fiabilité | observé | référence | horodatage (UTC) |
|---|---|---|---|---|---|
| `privacy-link-missing` | MOYENNE | observé | https://prestasoftware.com: no privacy link (looked for privacy / confidentialité / vie privée / privacidade / renseignements personnels / données personnelles / donnees personnelles / personal information / Loi 25 / Law 25 in anchor text or href) | bonne pratique | 2026-11-07T15:46:27Z |
| `dmarc-none` | FAIBLE | registre public : lu dans le DNS ou au registre du domaine, jamais sur le site | _dmarc.prestasoftware.com TXT: "v=DMARC1; p=none; rua=mailto:lps01@prestasoftware.com"; p=none; reports to mailto:lps01@prestasoftware.com | RFC 7489, section 6.3 (p=none ne demande aucune action; rua= nomme l'adresse des rapports) | 2026-11-07T15:46:35Z |
| `caa-missing` | INFORMATION | registre public : lu dans le DNS ou au registre du domaine, jamais sur le site | prestasoftware.com CAA: no CAA record | RFC 8659 (CAA) : lignes d'autorisation d'autorité de certification | 2026-11-07T15:46:27Z |
| `csp-weak-style` | INFORMATION | observé | https://prestasoftware.com: style-src allows 'unsafe-inline' | W3C Content Security Policy niveau 3 (sémantique de style-src) | 2026-11-07T15:46:27Z |

| règle | gravité | fiabilité | observé | référence | horodatage (UTC) |
|---|---|---|---|---|---|
| `ct-names-seen` | INFORMATION | registre public : lu dans le DNS ou au registre du domaine, jamais sur le site | prestasoftware.com CT names: www.prestasoftware.com; these names were not contacted | API certspotter avec repli crt.sh | 2026-11-07T15:46:27Z |
| `dns-host-named` | INFORMATION | registre public : lu dans le DNS ou au registre du domaine, jamais sur le site | prestasoftware.com NS: beau.ns.cloudflare.com, martha.ns.cloudflare.com; who to ask: CLOUDFLARENET | lignes NS et RDAP sur la première adresse A, via le fichier d'amorçage de l'IANA | 2026-11-07T15:46:27Z |
| `dnssec-off` | INFORMATION | registre public : lu dans le DNS ou au registre du domaine, jamais sur le site | prestasoftware.com DS: no DS record at the parent zone | RFC 4033-4035 (DNSSEC) : la ligne DS dans la zone parente indique une délégation signée | 2026-11-07T15:46:27Z |
| `mta-sts-missing` | INFORMATION | registre public : lu dans le DNS ou au registre du domaine, jamais sur le site | _mta-sts.prestasoftware.com TXT: no TXT record | RFC 8461 (MTA-STS) : ligne TXT à _mta-sts.<domaine> | 2026-11-07T15:46:27Z |
| `spf-names-left-services` | INFORMATION | registre public : lu dans le DNS ou au registre du domaine, jamais sur le site | prestasoftware.com TXT: "v=spf1 include:_spf.mx.cloudflare.net ~all"; names: _spf.mx.cloudflare.net | RFC 7208, sections 5.2 (include) et 6.1 (redirect) | 2026-11-07T15:46:35Z |

| règle | gravité | fiabilité | observé | référence | horodatage (UTC) |
|---|---|---|---|---|---|
| `third-parties-listed` | INFORMATION | observé | https://prestasoftware.com: analytics: none; ads_pixels: none; tag_managers: none; embeds: none; chat: none; other: static.cloudflareinsights.com | bonne pratique | 2026-11-07T15:46:27Z |
| `tls-rpt-missing` | INFORMATION | registre public : lu dans le DNS ou au registre du domaine, jamais sur le site | _smtp._tls.prestasoftware.com TXT: no v=TLSRPTv1 record | RFC 8460 (rapports SMTP TLS) : ligne TXT à _smtp._tls.<domaine> avec v=TLSRPTv1 | 2026-11-07T15:46:27Z |