CARDINAL SECURITY
YOUR SECURITY COMPASS

RAPPORT D'EXPOSITION NUMÉRIQUE

novaforge-industrie.fr

Date d'analyse : 05/06/2026

Synthèse exécutive

Cardinal Security a analysé l'exposition numérique de novaforge-industrie.fr à partir d'informations exclusivement publiques, sans aucun accès aux systèmes internes.

Le score d'exposition global est de **93/100 — CRITIQUE**. Plus le score est élevé, plus l'exposition au risque est importante.

Tableau de bord

Catégorie	Constat	Niveau
DMARC	Absent — usurpation d'email facilitée *Revue Cardinal : Levier d'usurpation le plus simple à exploiter, et le plus rapide à corriger.*	**MOYEN**

Détail des findings

Nom de domaine

Information	Valeur
Registrar	OVH SAS

APERÇU

■■ **Le domaine expire dans 45 jours et ne dispose pas de verrou de transfert (transfer lock)**

Sécurité email

Protocole	Valeur / Statut
SPF	v=spf1 include:_spf.google.com include:mailgun.org ~all

APERÇU

APERÇU

Empreinte réseau

Cartographie des adresses et réseaux sur lesquels vos services sont hébergés, reconstituée à partir des données publiques de routage Internet. Elle dessine le périmètre technique visible de l'extérieur.

Opérateur / réseau (AS)	Adresses concernées	Plage(s) d'adresses
AS16276 — OVH SAS	185.53.178.10, 185.53.178.22, 51.83.45.12	185.53.176.0/22, 51.83.0.0/16

Fuites de données

Vérification des emails de votre domaine dans les bases de données publiques de fuites (sites piratés, bases revendues). Un email compromis signifie que le mot de passe associé peut circuler sur Internet.

Email	Fuites	Sources
c*t@novaforge-industrie.fr**	**4**	LinkedIn, Dropbox, Adobe, Collection1

APERÇU

j*n@novaforge-industrie.fr**	**3**	LinkedIn, Twitter, Deezer
r*h@novaforge-industrie.fr**	**2**	Dropbox, Adobe

Typosquatting (6)

Domaine suspect	Type	IP
novaforge-industrle.fr	homoglyph	185.53.178.9

APERÇU

Sous-domaine
www.novaforge-industrie.fr

APERÇU

Documents & Interfaces exposés

Recherche automatisée des documents et interfaces de votre domaine accessibles publiquement sur Internet, sans mot de passe ni accès particulier.

Interfaces d'administration exposées

URL (cliquable)	Titre
https://admin.novaforge-industrie.fr/login	Portail d'administration — NovaForge

APERÇU

Documents PDF publics

URL (cliquable)	Titre
https://novaforge-industrie.fr/docs/tarifs-pro-2026.pdf	Tarifs professionnels 2026

APERÇU

URL (cliquable)	Titre
https://novaforge-industrie.fr/exports/clients-grands-comptes...	Clients grands comptes

Services exposés sur Internet

Équipements et services de votre organisation visibles publiquement sur Internet, tels qu'indexés par les moteurs de recherche spécialisés. Ces informations sont accessibles à n'importe quel attaquant sans aucune action particulière.

185.53.178.10 **remote.novaforge-industrie.fr**
OVH SAS — France

Port	Service / Produit	Risque
443/tcp	Microsoft IIS 8.5	

APERÇU

CVEs détectées : CVE-2019-0708

185.53.178.22 **ftp.novaforge-industrie.fr**
OVH SAS — France

Port	Service / Produit	Risque
21/tcp	vsftpd 2.3.4 FTP — transfert de fichiers en clair (port 21), identifiants non chiffrés	ÉLEVÉ

APERÇU

Exposition via repository GitHub

Recherche de votre domaine dans le code public publié sur GitHub. Un développeur peut, par erreur, publier un fichier de configuration contenant des identifiants liés à votre entreprise.

Ces résultats sont des PISTES à vérifier manuellement : la simple présence du domaine près d'un mot-clé ne prouve pas une fuite réelle.

Mots de passe à proximité du domaine (8 au total sur GitHub)

Dépôt / fichier (cliquable)	Analyse & extrait
novaforge-dev/legacy-scripts › deploy/config.env 2026-02-14	**[ÉLEVÉ]** Fichier de configuration contenant des identifiants SMTP en clair (utilisateur + mot de passe). `SMTP_USER=contact@novaforge-industrie.fr SMTP_PASSWORD=Nov@Forge2023!`

APERÇU

Dépôt / fichier (cliquable)	Analyse & extrait
novaforge-dev/mobile-app › app/constants.js 2026-04-01	**[ÉLEVÉ]** Clé d'API de paiement (Stripe, live) potentiellement exposée dans une application mobile. `const API_BASE='https://api.novaforge-industrie.fr'; const STRIPE_KEY='sk_live_5lHxxxxxREDACTED';`

Scénario d'attaque

Voici comment un attaquant pourrait concrètement exploiter votre exposition, à partir des éléments détectés dans ce rapport :

L'attaquant commence par recenser vos adresses email professionnelles, dont plusieurs apparaissent déjà dans des fuites de données publiques. Faute de protection DMARC, il usurpe votre nom de domaine et adresse à votre

APERÇU

Déroulé de l'attaque

1. Reconnaissance
Collecte des emails exposés et des fuites de données.

2. Usurpation email
Faux email de la direction, DMARC absent.

APERÇU

Plan d'action prioritaire

Priorité	Action recommandée	Pour qui	Effort · Coût	Délai
ÉLEVÉ	**Fermer l'accès RDP exposé (serveur 185.53.178.10)** Le Bureau à distance (RDP, port 3389) de remote.novaforge-industrie.fr (185.53.178.10) est ouvert sur Internet. Retirez-le d'Internet et n'y accédez plus que via un VPN (tunnel privé chiffré) avec double authentification. **Pourquoi :** Un RDP exposé est l'une des premières portes d'entrée des rançongiciels.	Prestataire IT	Faible · Gratuit	Immédiat

APERÇU

CARDINAL SECURITY

YOUR SECURITY COMPASS

VOTRE BOUSSOLE CYBERSÉCURITÉ

Pour toute question relative à ce rapport, contactez-nous.

Web : www.cardinalsecurity.fr

Adresse : 66 avenue des Champs-Élysées, 75008 Paris