formind

Security
for business
performance

CERT Formind

RFC 2350

Diffusion externe

TLP:CLEAR

En cas d'incident de sécurité
fir@formind.fr – 01 81 89 30 02

Date : 05/11/2024

Version : 1.2

Sommaire

1 A propos de ce document

Ce document contient une description du CERT Formind, tel que spécifié par la RFC2350.

1.1 Date de dernière mise à jour

La version actuelle de ce document est la v.1.2 publiée le 05 novembre 2024.

1.2 Liste de diffusion des notifications

Il n'existe pas de liste de distribution pour les notifications.

1.3 Lieu de distribution de ce document

La dernière version de ce document est publiée sur le site internet de Formind à l'adresse : https://www.formind.fr/expertises/soccert/

1.4 Authenticité de ce document

Ce document a été signé avec la clé PGP du CERT Formind.
La clé publique du CERT Formind est disponible sur le site internet du CERT Formind à cette adresse : https://www.formind.fr/expertises/soccert/

1.5 Identification du document

Titre : "CERT Formind - RFC2350 - v1.2"
Version : 1.2
Date de publication : 05 novembre 2024.
Expiration : ce document est valable jusqu'à la publication d'une nouvelle version.

2 Informations sur le CERT Formind

2.1 Nom de l'équipe

CERT Formind

2.2 Adresse

CERT Formind
43 rue Camille Desmoulins
92 130 Issy les Moulineaux
France

2.3 Zone de temps

CET/CEST : Paris (GMT+01:00 ou GMT+02:00 en heure d'été)

2.4 Numéro de téléphone

+33 1 81 89 30 02

2.5 Numéro de fax

N/A.

2.6 Autre moyen de contact

Les informations de contact de Formind sont disponibles sur le site internet de Formind à l'adresse : https://www.formind.fr/contactez-nous/

2.7 Adresse électronique

cert@formind.fr

2.8 Clé publique et information sur le chiffrement

Les informations de la clé PGP du CERT Formind sont :

- KeyID : 0x462AD29B
- Fingerprint : A2C4DCFFAC8221FCCAB544CE933C5D1B462AD29B

La clé publique du CERT est disponible sur le site de Formind à l'adresse :
https://www.formind.fr/expertises/soccert/

2.9 Membre de l'équipe

Le CERT Formind est dirigé par le Directeur D&T-SOC-CERT. Il est constitué des personnes aux postes suivants :

- Responsable VOC,
- Responsable SOC,
- Responsable FIR,
- Responsable Audits.

2.10 Heure d'ouverture

Le CERT Formind est ouvert de 9h à 18h du lundi au vendredi hors jours fériés.

Le service de réponse à incident porté par la FIR Formind assure une astreinte disponible 24h/24 7j/7.

2.11 Point de contact pour les abonnés au CERT Formind

Les abonnés du CERT Formind peuvent contacter les différents services via les adresses de messagerie électronique suivantes :

- VOC : voc@formind.fr
- SOC : soc@formind.fr

- FIR : fir@formind.fr

En cas de cyber attaque, il est recommandé d'utiliser le numéro d'astreinte de la FIR :
+33 1 81 89 30 02

2.12 Autres informations

Des informations complémentaires sont disponibles sur le site internet de Formind via l'adresse : https://www.formind.fr/

3 Charte

3.1 Ordre de mission

Le CERT Formind est un CERT privé offrant divers services aux entreprises de toutes les tailles et de tous les secteurs d'activités.

Les missions du CERT Formind sont l'anticipation, la détection et la réponse à incident. Ces missions sont portées par les services :

- VOC : Veille, OSINT & CTI
- SOC : Security Operations Center
- FIR : Force d'Intervention Rapide
- Audits techniques

Les objectifs du CERT Formind sont :

- Mener une veille active sur les vulnérabilités et l'évolution des modes opératoires.
- Partager des informations actionnables sur les menaces, au travers de rapports de CTI, d'indicateurs de compromission et d'attaque, et de règles de détection.
- Détecter les vulnérabilités sur les réseaux et systèmes des abonnés.
- Notifier les abonnés des vulnérabilités, menaces et attaques pouvant les impacter.
- Analyser l'empreinte numérique d'une entreprise ou d'une personne d'intérêt sur le Clear, Deep et Dark Web.
- Détecter et qualifier les alertes de sécurité sur les Systèmes d'Information des abonnés.
- Réaliser les investigations numériques lors de cyberattaques.
- Piloter la réponse à incident et aider les victimes de cyberattaques à revenir en condition de sécurité.
- Accompagner à la gestion de crise cyber.

3.2 Entités bénéficiant du service

Les entreprises françaises et internationales peuvent bénéficier des services du CERT Formind.

Formind profite en interne du service du CERT pour sa propre activité.

4 Politiques

4.1 Types d'incidents et niveau d'intervention

Le CERT Formind au travers du service de la Force d'Intervention Rapide (FIR) offre des capacités d'assistance en cas d'incident cyber. La FIR intervient à trois niveaux :

- la gestion de crise : permettant aux victimes de cyberattaques d'avoir un accompagnement à la mise en place de l'organisation de crise,
- le pilotage de la réponse : permettant le suivi des plans d'actions pour un retour en condition de sécurité rapide,
- les investigations numériques : permettant la compréhension du vecteur d'attaque et la mise en place des contre-mesures.

La FIR Formind a la capacité d'intervenir sur tout type d'incident : rançongiciel, hameçonnage, déni de service, menace interne, ...

La FIR Formind est disponible du lundi au vendredi de 9h à 18h pour toutes les organisations et offre une assistance d'astreinte pour ses abonnés y ayant souscrit.

4.2 Coopération, interaction et divulgation d'informations

Les informations sont transmises en fonction de son marquage TLP et du principe du « besoin d'en connaitre ». Le CERT Formind applique le protocole Traffic Light Protocol (TLP) tel que défini dans la version 2.0 du FIRST : https://www.first.org/tlp/.

Les informations relatives à un incident de cyber sécurité ne sont pas partagées sans un accord écrit préalable du commanditaire.

4.3 Communication et authentification

Le moyen de communication privilégié pour le CERT Formind est la messagerie électronique. En cas d'urgence, il est toutefois recommandé de contacter le CERT par téléphone.

Les informations sensibles sont chiffrées avant d'être transmises. Le CERT Formind utilise PGP et Zed! pour garantir la confidentialité et l'intégrité des données échangées.

5 Service

5.1 Activités réactives

L'objectif principal du CERT Formind est de venir en aide aux organisations victimes d'une cyberattaque.

Triage

Le CERT Formind intervient pour identifier le périmètre impacté par l'attaque ainsi que les équipements nécessitant une investigation numérique approfondie. Il assure également

l'acquisition des preuves et artefacts indispensables à la réalisation de ces investigations, garantissant ainsi une analyse précise et pertinente.

Coordination
Le CERT Formind dispose de pilotes techniques, permettant de coordonner les actions d'isolation, d'investigation et de remédiation. Le CERT Formind a aussi la capacité d'accompagner les victimes à mettre en place l'organisation de crise.

Résolution
Grâce aux les investigations numériques, les informations du renseignement sur la menace et l'OSINT, le CERT Formind a la capacité d'établir un plan d'actions efficient garantissant un retour en condition de sécurité rapide. Le CERT Formind fournit un rapport d'incident détaillé sur les investigations réalisées, ainsi qu'une liste de recommandations pour augmenter le niveau de sécurité du SI.

5.2 Activités proactives

5.2.1 Informations et alertes
Le CERT Formind à travers son service VOC réalise une veille active sur les vulnérabilités et les menaces cyber. Il notifie ses abonnées via des bulletins de veille disponible sur leur portail client et les envoie par messages électroniques. L'objectif est d'anticiper et de prévenir un risque cyber par des recommandations adaptées et la mise en œuvre d'actions correctives ou palliatives.

5.2.2 Audit et évaluation de la sécurité
Le CERT Formind, à travers son équipe d'audits techniques, a la capacité de réaliser des tests d'intrusion, des Red Team, de l'audit de code et de configuration. Ceci dans l'objectif de délivrer des recommandations de sécurisation et ainsi réduire les risques de compromission du SI.

5.2.3 Gestion de la vulnérabilité
Le CERT Formind adopte une stratégie de gestion des vulnérabilités à trois niveaux :

1. Détecter les vulnérabilités exploitables sur un parc afin de mieux connaitre les faiblesses du SI et les corriger pour en empêcher l'exploitation par des acteurs malveillants.
2. Acquérir une visibilité complète sur l'ensemble des actifs et applications, qu'ils soient internes ou externes, ceci afin de ne plus laisser l'opportunité aux attaquants d'exploiter les angles morts d'un SI.
3. Optimiser le workflow de gestion des vulnérabilités afin de réduire le temps de traitement des opérations d'application des correctifs de vulnérabilités présentes sur un parc et ainsi minimiser la durée d'exposition des actifs et applications.

5.2.4 Renseignement sur la menace
Le CERT Formind suit les principaux acteurs de la menace et groupes d'attaquant pour être en mesure de :

- Notifier ses abonnés des cyberattaques en cours et des vulnérabilités connues activement exploitées pouvant les impacter.
- Informer sur l'évolution des menaces, tactiques, techniques et procédures et les tendances.
- Proposer un plan d'actions basé sur des mesures correctives ou palliatives vis-à-vis du contexte.
- Communiquer des indicateurs de compromission et d'attaque.
- Apporter un support dans la mise en place d'une stratégie de détection adaptées par rapport à ses observations.

5.2.5 Détection d'incident

Le SOC de Formind, intégré au sein du CERT, joue un rôle clé dans la protection des systèmes d'information. Son activité se concentre sur la surveillance continue, l'analyse des menaces et la gestion des alertes de sécurité. Le SOC aide à se protéger des cyberattaques en déployant des solutions de détection et en renforçant les mesures de sécurité.

6 Formulaire de notification d'incidents

Le CERT Formind ne dispose pas d'un formulaire de notification d'incident. Le CERT peut être notifié d'un incident par courriel ou par téléphone. Les informations minimales à fournir sont :

- Un point de contact (nom, prénom, numéro de téléphone, adresse électronique) ;
- La date de détection de l'incident ;
- La typologie de l'incident ;
- Une description de l'incident ;
- Le type et le nombre d'actifs impactés ;
- Les actions déjà réalisées pour contenir l'incident.

7 Décharge de responsabilité

Bien que toutes les précautions soient prises dans la préparation des informations, notifications et alertes, le CERT Formind se décharge de toute responsabilité pour les erreurs, omissions ou pour les dommages résultant de l'utilisation des informations contenues.

En cas d'incident de sécurité
fir@formind.fr – 01 81 89 30 02

formind

Security
for business
performance

www.formind.fr