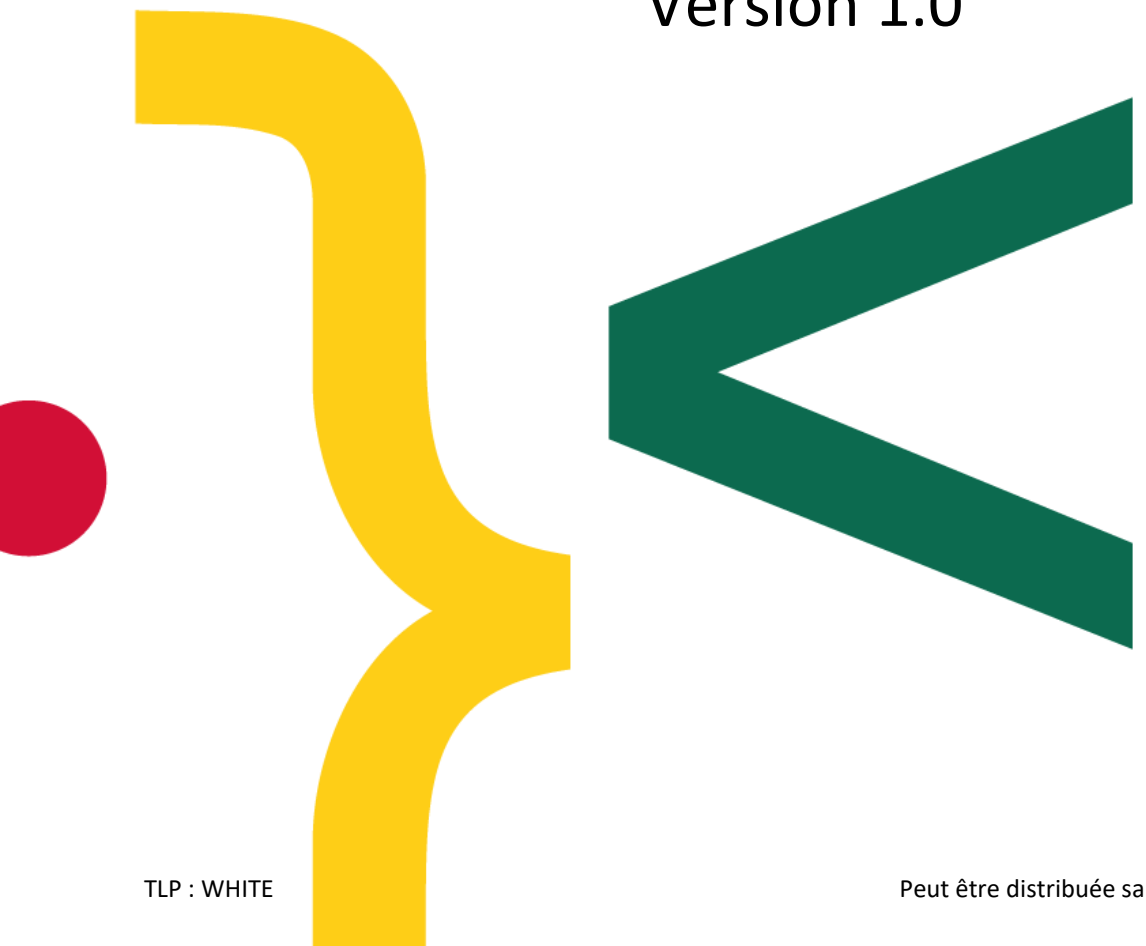
Description du CERT.tg

RFC 2350

Version 1.0



1. A propos de ce document

Ce document contient la description du CERT.tg tel que spécifié par le RFC 2350.
Il fournit des informations de base sur le CERT.tg, ses moyens de communication ainsi que ses rôles et responsabilités.

1.1. Date de dernière mise à jour

Ce document (Version 1.0) est publié le 07 Décembre 2020

1.2. Liste de diffusion et de notification

CERT.tg n'utilise pas de liste de distribution pour informer sur les changements liés à ce document. Cette page est mise à jour sur le lien spécifié dans la section 1.3.

1.3. Lieux de distribution de ce document

La présente version de ce document peut être trouvé sur le site Web du CERT.tg sur le lien suivant : cert.tg/about-us/CERT-tg-RFC-2350-FR

1.4. Authenticité de ce document

Ce document a été signé avec la clé PGP du CERT.tg.
Veuillez consulter la section 2.8 de ce document pour plus d'informations.

1.5. Identification du document

Titre : CERT-tg_RFC2350_FR
Version : 1.0
Date du document : 07-12-2020
SHA-256
Durée de validité : ce document est valide jusqu'à ce qu'il soit remplacé par une version ultérieure

2. Point de contact

Cette section décrit comment contacter le CERT.TG.

2.1. Nom de l'équipe

CERT TOGO, CERT National de la République Togolaise
Nom court : CERT.tg

2.2. Adresse

Ministère de l'Economie Numérique et de la Transformation Digitale
Avenue Abdoulaye Fadiga
07 BP 13215 - Lomé, Togolaise

2.3. Fuseau Horaire

UTC

2.4. Numéro de Téléphone

Fixe : +228 22 53 59 80 / Mobile : +228 70 54 93 25

2.5. Fax

N/A

2.6. Autres moyens de contacts

N/A

2.7. Adresse électronique

Renseignements généraux : contact@cert.tg
Signaler un incident de cybersécurité : incidents@cert.tg

2.8. Clé publique et informations de chiffrement

PGP est utilisé pour les échanges avec CERT.tg
- Identifiant de la clé : 0x2C5D9DBA
- Empreinte de la clé : 48D0 0B2C 6163 8539 4C43 6927 8F35 B74A 2C5D 9DBA

La clé PGP publique est disponible sur ce lien et peut être retrouvée sur les serveurs publics de clé.

2.9. Membres de l'équipe

La liste des membres de l'équipe CERT.tg n'est pas accessible au public.
Certaines informations sur les membres peuvent être divulguées sur demande.

2.10. Autres informations

Veuillez consulter notre site Web www.cert.tg pour plus d'informations sur CERT.tg

2.11. Point de contact des clients

Pour des renseignements généraux : contact@cert.tg
Pour les incidents de cybersécurité : incidents@cert.tg
Nous encourageons nos clients à utiliser notre clé cryptographique pour garantir l'intégrité et la confidentialité de l'information.

En cas d'impossibilité d'utilisation du courrier électronique (ou pour des raisons de sécurité), veuillez contacter le CERT.tg par téléphone :
Fixe: +228 22 53 59 80
Mobile: +228 70 54 93 25
CERT.tg est joignable 24h/24 et 7j/7.

3. Charte

3.1. Ordre de mission

CERT.tg est le centre national de réponse aux incidents de cybersécurité (CERT) en République togolaise. La mission du CERT.tg est d'identifier, analyser, et mitiger les menaces ciblant l'Etat togolais, les administrations, les agences publiques, les entreprises publiques et privées et les citoyens.
CERT.tg contribue à la protection du cyberespace togolais.

3.2. Périmètre d'intervention

Le périmètre d'intervention est composé de l'ensemble de la République togolaise :

- Les ministères, administrations et services de l'Etat ;
- Les opérateurs de services essentiels et les opérateurs d'infrastructures critiques tels que définis dans la loi Togolaise ;
- Autres acteurs clés dans les secteurs sensibles ;
- L'ensemble des citoyens de la République togolaise.

3.3. Parrainage et relations

République togolaise
Ministère de l'Economie Numérique et de la Transformation Digitale (MENTD)
Ministère de la Sécurité et de la Protection Civile (MSPC)
Ministère de l'Economie et des Finances (MEF)
Agence Nationale de Cybersécurité (ANCy)
Autorité de Régulation des Communications Electronique et des Postes (ARCEP)
Cyber Defense Africa (CDA)

3.4. Autorité

La création du CERT.tg est mandaté par le "Décret 2019-098 portant création, attribution et organisation de la société CDA" qui définit les compétences et l'autorité du "CERT.tg".
CERT.tg est opéré par Cyber Defense Africa S.A.S (CDA) en tant que service délégué par l'Agence Nationale de Cybersécurité (ANCy).
CDA est sous la tutelle du MENTD, du MSPC et du MEF.
L'ANCY est sous la tutelle de la Primature, du MENTD, MSPC, MEF, Ministère des Armées (MA) Ministère de la Justice (MJ) et de la Présidence de la République.

4. Politiques

4.1. Types d'incidents et niveaux de supports

CERT.tg est autorisé à coordonner et à traiter tous les types d'incidents de sécurité informatique qui ciblent ou menacent de cibler en République togolaise.
Le niveau de support fournit par le CERT.tg peut varier en fonction du type d'incident, de sa sévérité, du nombre d'utilisateurs affecté par l'incident et des ressources disponibles pour le traiter.

4.2. Coopération, interaction et divulgation d'informations

Toutes les informations reçues par CERT.tg relatives aux incidents de cybersécurité sont considérées comme confidentielles et ne sont utilisées que pour résoudre les incidents et prévenir d'autres incidents. Les informations sensibles (telles que les données personnelles, les configurations système) ou qui peuvent être nuisibles, sont traitées dans un environnement sécurisé et chiffré, si elles doivent être transmises sur un environnement non sécurisé.
Les informations soumises au CERT.tg peuvent être diffusées aux parties intéressées, telles que d'autres équipes CERT/CSIRT, nos partenaires technologiques, les administrateurs des ressources affectées, d'autres entités faisant partie de l'écosystème national de cybersécurité, sur la base du « need to know », aux seules fins de la gestion des incidents (c'est-à-dire dans la mesure nécessaire pour identifier et atténuer la menace). Aucune information d'identification personnelle n'est échangée, sauf autorisation expresse et préalable.
Veuillez consulter notre déclaration de confidentialité sur www.cert.tg/privacy-statement/

4.3. Communication et authentification

La méthode de communication préférée est le courrier électronique.

1. Pour les informations à faible sensibilité, des méthodes non chiffrées telles que les e-mails ou les téléphones peuvent être utilisées.
2. Toutes les informations sensibles partagées sur CERT.tg doivent être chiffrées avec notre clé PGP publique détaillée dans la section 2.8.

5. Services

5.1. Réponse aux incidents

CERT.tg fournit les services de réponse aux incidents de cybersécurité 24h/24 et 7J/7 dans les domaines suivants :

5.1.1. Triage

- Évaluation des rapports d'incidents : interprétation des incidents reportés, hiérarchisation et liaison avec les incidents et tendances en cours ;
- Vérification : détermination si un incident s'est réellement produit et sa portée.

5.1.2. Coordination

- Catégorisation des informations : Catégorisation des informations relatives à l'incident (fichiers journaux d'évènements, coordonnées, etc.) conformément à la politique de divulgation des informations.
- Coordination : notification des autres parties impliquées sur la base du « need to know », conformément à la politique de divulgation d'informations.

5.1.3. Résolution

- Assistance technique : Cela peut inclure l'analyse des systèmes compromis.
- Eradication : Élimination de la cause d'un incident de sécurité (la vulnérabilité exploitée), et de ses effets.
- Récupération : aide à restaurer les systèmes et services affectés à leur état avant l'incident de sécurité.

5.2. Activités proactives

5.2.1. Annonces

Les annonces comprennent des alertes de sécurité, des avertissements de vulnérabilité, des menaces et incidents de sécurité ainsi que des indicateurs de compromission. De telles annonces informent les citoyens et les entreprises du périmètre d'intervention du CERT.tg des nouveautés en matière de cybercriminalité et de cybersécurité. Les annonces permettent aux destinataires de protéger leurs systèmes et réseaux contre les problèmes nouvellement découverts avant qu'ils ne puissent être exploités.

5.2.2. Veille technologique

CERT.tg surveille et observe les nouveaux développements techniques, les activités des intrus et les tendances connexes pour aider à identifier les menaces futures. Les sujets examinés peuvent être élargis pour inclure des décisions juridiques et législatives, les menaces sociales ou politiques et les nouvelles technologies.

5.2.3. Sensibilisation

CERT.tg fournit un ensemble complet et facile à trouver d'informations utiles qui aident à améliorer le niveau de sécurité des entreprises et des citoyens togolais.

5.2.4. Formations

Ce service consiste à informer les citoyens togolais, les écoles / universités et les organisations sur les questions de sécurité informatique à travers des séminaires, des ateliers, des cours et des tutoriels.

5.2.5. Audits et évaluations de sécurité

CERT.tg fournit une revue et une analyse détaillées de l'infrastructure de sécurité des entreprises et administrations, en fonction des exigences définies par loi togolaise, l'ANCy ou en conformité avec des normes et standards internationaux.

5.2.6. Rapports périodiques

CERT.tg prépare et publie des rapports périodiques sur ses opérations et la cybersécurité au Togo.

6. Formulaire de déclaration d'incidents

Aucun formulaire spécifique n'est nécessaire pour signaler les incidents de sécurité par e-mail ou par téléphone. Lors du signalement d'un incident sur le site CERT.tg, certaines informations clés (coordonnées de contact, description de l'incident, les mesures de remédiations déjà prises le cas échéant, etc.) sont obligatoires. Veuillez consulter www.cert.tg/report-incident.

7. Clause de non-responsabilité

Bien que toutes les précautions soient prises dans la préparation des informations, notifications et alertes, CERT.tg n'assume aucune responsabilité pour les erreurs ou omissions, ou pour les dommages résultant de l'utilisation des informations fournies.