MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

Direction du Renseignement et
de la Sécurité de la Défense

Description

CERT [ED]

Computer Emergency Response Team
Entreprises de Défense

RFC 2350

1er février 2024

Ministère des Armées
60, boulevard du général Martial VALIN
CS 21 623 - Case 44
75 509 PARIS CEDEX 15

1. A PROPOS DE CE DOCUMENT

Ce document est une description des principales caractéristiques du CERT [ED] (Computer Emergency Response Team – Entreprises de Défense), conformément au format RFC 2350 défini par l'IETF *(Internet Engineering Task Force).*

1.1. Dernière mise à jour

Ce document est la version 1.2 du 1/2/2024.

1.2. Notification des modifications

Il n'existe pas de liste de notification des modifications.

Les demandes d'informations sur les modifications doivent être adressées à l'adresse mail du CERT [ED] : cert-drsd.contact.fct[/at]def.gouv.fr

1.3. Lieu de publication de ce document

La version actuelle de ce document est disponible à l'adresse : www.drsd.defense.gouv.fr/cert-ed.

1.4. Authenticité de ce document

CERT [ED]

1.5. Identifiant du document

- Titre : CERT-ED_RFC_2350.pdf
- Version : 1.2
- Date : 1/2/2024
- Expiration : ce document est valide jusqu'à ce qu'il soit remplacé par une version ultérieure. Veuillez-vous assurer d'utiliser la dernière version.

2. INFORMATIONS DE CONTACT

2.1. Nom de l'équipe

Nom complet : Centre de réponse à incident des Entreprises de Défense

Nom abrégé : CERT [ED]

2.2. Adresse

Ministère des Armées
60, boulevard du général Martial VALIN
CS 21 623 – Case 44
75 509 PARIS CEDEX 15, FRANCE

2.3. Fuseau horaire

CET/CEST : Europe/Paris

2.4. Numéro de téléphone

Point de contact téléphonique (JO/HO) : 0 805 046 300

2.5. Numéro de fax

N/A

2.6. Autres moyens de communication

N/A

2.7. Adresse email

Les signalements d'incidents doivent être envoyés à l'adresse :

cert-drsd.contact.fct[/at]def.gouv.fr

2.8. Clés publiques et moyens de chiffrement

CERT [ED]

	Point de contact
Email	cert-drsd.contact.fct[/at]def.gouv.fr
Identifiant clé	A99FF908
Empreinte	BC0E E7D0 16F0 4223 5642 EA1B C70E DC8A A99F F908
Expiration	09-07-2027

La clé OpenPGP publique est disponible à l'adresse :

https://www.drsd.defense.gouv.fr/cert-ed/

2.9. Membres de l'équipe

L'équipe du CERT est constituée d'ingénieurs et techniciens spécialisés en matière de cyberdéfense/cybersécurité et de développeurs logiciels pour les fonctions support.

Pour des raisons de confidentialité, la liste des membres du CERT [ED] n'est pas disponible publiquement.

2.10. Autres informations

Plus d'informations sur le CERT [ED] sont disponibles à l'adresse www.drsd.defense.gouv.fr/cert-ed

2.11. Point de contact

Le mode de communication privilégié est la messagerie électronique (cf. 2.7). L'utilisation de la clé OpenPGP est recommandée pour assurer l'intégrité et la confidentialité des échanges.

Horaires d'ouverture habituels : Lundi-Vendredi, 9h-17h (hors jours fériés en France)

3. CHARTE

3.1. Mission

La mission du CERT [ED] consiste à contribuer à la sécurité des systèmes informatiques des entreprises de défense. Le CERT[ED] est chargé de contribuer à la protection, à la prévention et à la réponse aux attaques informatiques. En tant que CERT, il participe activement à l'échange d'informations liées à la cybersécurité, au sein de la sphère « défense » et avec ses partenaires de la communauté des CSIRTs.

Le CERT [ED] accompagne notamment les entreprises de défense dans le cadre de la réponse aux incidents de cybersécurité.

Les missions du CERT couvrent :

- La prévention des incidents de sécurité en développant la sensibilisation à la cybersécurité,
- La gestion des incidents en coordonnant, centralisant et identifiant les cyber-incidents,
- Le partage d'informations d'intérêt pour le secteur.

3.2. Périmètre d'intervention

Le périmètre d'intervention du CERT [ED] couvre les entreprises de défense et/ou organismes dont la Direction du Renseignement et de la Sécurité de la Défense (DRSD) assure la protection au titre de ses missions régaliennes.

3.3. Parrainage et/ou affiliation

Le CERT [ED] est intégré à la DRSD, subordonnée au ministre des armées.

3.4. Autorité

Le CERT [ED] agit sous l'autorité du Directeur de la DRSD.

4. STRATEGIES

4.1. Types d'incidents et niveau de soutien

Le CERT [ED] traite tous les types d'incidents de cybersécurité qui surviennent ou menacent de survenir au sein du périmètre défini supra.

Le niveau d'assistance fourni par le CERT [ED] varie en fonction :

- du type et de la gravité de l'incident,
- des systèmes concernés,
- de l'impact potentiel de l'incident,
- de la taille de la communauté d'utilisateurs affectée,

4.2. Coopération, interaction et divulgation d'information

Le CERT [ED] échange des informations avec les acteurs de la chaine de cyberdéfense nationale dans le respect des règlementations en vigueur.

Par défaut, aucune information liée aux incidents traités n'est publiée ou communiquée à un tiers, sauf si la loi française l'exige. En revanche le CERT [ED] peut communiquer à titre préventif sur les menaces et les techniques, tactiques et procédures employés par certains groupes d'attaquants adverses.

4.3. Communication et authentification

Le moyen de communication privilégiée est la messagerie électronique.

Pour les échanges d'informations sensibles et les communications sécurisées, le CERT [ED] met à disposition sur son site une clé OpenPGP publique (cf. section 2.8). Dans la mesure du possible, l'emploi de cette clé est à privilégier.

5. SERVICES

Le CERT [ED] a pour vocation d'apporter un soutien dans la prévention et la gestion des incidents cyber.

5.1. Sensibilisation

Le CERT [ED] partage ses connaissances et son expérience en sensibilisant les entreprises de défense qui le souhaitent sur les sujets de cyber sécurité. Directement au sein des entreprises ou lors de séminaires dédiés rassemblant des entreprises, une action de sensibilisation peut être menée en visant à faire connaître les bonnes pratiques, les recommandations SSI et l'écosystème cyber français (cybermalveillance.gouv.fr, ANSSI).

5.2.. Veille en vulnérabilités

Le CERT [ED] est en mesure de veiller les annonces sur les vulnérabilités concernant des logiciels ou matériels spécifiques et d'alerter les parties concernées. En fonction des éléments fournis, le CERT[ED] est en capacité d'assurer une veille dédiée et adaptée à chaque entreprise qui en exprime le besoin.

5.3. Gestion de la réponse à incident

Il accompagne les administrateurs et exploitants de systèmes dans la gestion des aspects techniques et organisationnels des incidents. En particulier, il fournit une assistance ou des conseils pour les aspects suivants :

- Catégorisation des incidents,
- Coordination des incidents.

5.4. Coopération

Le CERT [ED] coopère au niveau national et régional en :

- Echangeant avec les acteurs cyber du ministère des Armées sur les risques, les menaces, les vulnérabilités et incidents identifiés pour son périmètre de responsabilité,
- Echangeant avec les autres services de l'Etat, autorités compétentes et autres CERT/CSIRT si cela s'avère utile, suivant le principe du besoin d'en connaître,
- Facilitant les échanges avec les autres entités potentiellement impactées,
- Tirant et partageant les enseignements liés à l'incident.

6. FORMULAIRE DE DECLARATION D'INCIDENT

Le signalement des incidents de sécurité est basé sur une procédure dédiée et des formulaires disponibles sur le site internet du CERT.

7. DECHARGE DE RESPONSABILITE

Bien que toutes les précautions soient prises dans l'élaboration des notes d'informations, notifications, alertes ou assistance dans le cadre de la « réponse à incidents », le CERT [ED] ne saurait être tenu pour responsable des erreurs ou omissions ou des dommages pouvant résulter de l'utilisation des informations qu'ils contiennent ou des actions entreprises sur les systèmes.

_____FIN DE DOCUMENT_____