**Les problèmes de sécurité**

**Modifier cette page**

Ce document explique comment les problèmes de sécurité de Carbone area sont gérés par l'équipe principale de Carbone area.

**Signaler un problème de sécurité**

Si vous pensez avoir trouvé un problème de sécurité dans Carbone area, n'utilisez pas le bug tracker et ne le publiez pas publiquement. Au lieu de cela, tous les problèmes de sécurité doivent être envoyés à **accueil@carbone-area.com**. Les e-mails envoyés à cette adresse sont transmis à la liste de diffusion privée de l'équipe principale de Carbone area.

**Ne sont pas considérés comme des problèmes de sécurité :**

* Problèmes détectés dans les outils de débogage non activés en production.
* Problèmes détectés dans les classes de test.
* Correctifs de sécurité comme l'énumération des routes, les limitations de connexion, les attaques par déni de service, etc.

L'équipe principale a la décision finale quant aux problèmes considérés comme des vulnérabilités de sécurité.

**Primes pour les bogues de sécurité**

Carbone area est un projet Open-Source où la plupart du travail est effectué par des bénévoles. Nous apprécions les efforts pour trouver des problèmes de sécurité et les signaler de manière responsable, mais nous ne sommes actuellement pas en mesure de payer des primes de bogues.

**Processus de résolution**

1. **Confirmation de la vulnérabilité**
2. **Développement d'un correctif**
3. **Obtention d'un identifiant CVE sur mitre.org**
4. **Rédaction d'une annonce de sécurité**
   * Titre avec "Communication de sécurité"
   * Description de la vulnérabilité
   * Versions concernées
   * Exploits possibles
   * Correction/mise à niveau/contournement
   * Identifiant CVE
   * Crédits
5. **Envoi du correctif et de l'annonce au journaliste pour examen**
6. **Application du correctif à toutes les versions maintenues de Carbone area**
7. **Publication de l'annonce sur le blog officiel Carbone area (catégorie "Security Advisories")**
8. **Mise à jour de la base de données des avis de sécurité publique**

**Pas de publication de versions avec des problèmes de sécurité le week-end**

**Confidentialité pendant la résolution**

**Collaboration avec des projets open source en aval**

* L'équipe de sécurité Carbone area informe les équipes de sécurité des projets en aval.
* Un référentiel Git privé est créé pour faciliter la collaboration.
* Les personnes ayant accès au référentiel travaillent sur une solution.
* Les projets impliqués collaborent pour trouver une date de sortie commune.

**Gravité du problème**

Un score sur 15 est converti en un niveau de gravité : Faible, Moyen, Élevé, Critique ou Exceptionnel.

**Complexité de l'attaque**

Score de 1 à 5 selon la complexité d'exploitation de la vulnérabilité.

**Impact**

Score de 0 à 6 selon l'impact de la vulnérabilité.

**Projets concernés**

Score de 1 à 4 selon le nombre de projets affectés.

**Totaux des scores**

* Complexité d'attaque : 1 - 5
* Impact : 1 - 6
* Projets concernés : 1 à 4

**Niveaux de gravité**

* Faible : 1 - 5
* Moyen : 6 - 10
* Élevé : 11 - 12
* Critique : 13 - 14
* Exceptionnel : 15

**Security Issues**

**Edit this page**

This document explains how security issues in Carbone area are handled by the Carbone area core team.

**Reporting a security issue**

If you believe you have found a security issue in Carbone area, do not use the bug tracker or publish it publicly. Instead, all security issues should be sent to **accueil@carbone-area.com**. Emails sent to this address are forwarded to the private mailing list of the Carbone area core team.

**The following are not considered security issues:**

* Issues found in debugging tools that are never enabled in production.
* Issues found in test classes.
* Security hardening fixes such as route enumeration, connection throttling, denial-of-service attacks, etc.

The core team has the final decision on which issues are considered security vulnerabilities.

**Security bug bounties**

Carbone area is an Open-Source project where most of the work is done by volunteers. We appreciate the efforts to find security issues and report them responsibly, but we are currently not able to pay bug bounties.

**Resolution process**

1. **Confirmation of the vulnerability**
2. **Development of a patch**
3. **Obtaining a CVE identifier on mitre.org**
4. **Writing a security advisory**
   * Title with "Security Advisory"
   * Description of the vulnerability
   * Affected versions
   * Possible exploits
   * Mitigation/upgrade/workaround
   * CVE identifier
   * Credits
5. **Sending the patch and advisory to the reporter for review**
6. **Applying the patch to all maintained versions of Carbone area**
7. **Publishing the advisory on the Carbone area official blog (category "Security Advisories")**
8. **Updating the public security advisories database**

**No release of versions with security issues on weekends**

**Confidentiality during resolution**

**Collaboration with downstream open source projects**

* The Carbone area security team notifies the security teams of downstream projects.
* A private Git repository is created to facilitate collaboration.
* People with access to the repository work on a solution.
* The involved projects collaborate to find a common release date.

**Severity of the issue**

A score out of 15 is converted to a severity level: Low, Medium, High, Critical, or Exceptional.

**Attack complexity**

Score from 1 to 5 depending on the complexity of exploiting the vulnerability.

**Impact**

Score from 0 to 6 depending on the impact of the vulnerability.

**Projects affected**

Score from 1 to 4 depending on the number of projects affected.

**Total scores**

* Attack complexity: 1 - 5
* Impact: 1 - 6
* Projects affected: 1 to 4

**Severity levels**

* Low: 1 - 5
* Medium: 6 - 10
* High: 11 - 12
* Critical: 13 - 14
* Exceptional: 15