



BULLETIN DE SECURITE

Titre	Vulnérabilité critique affectant le logiciel de surveillance réseau Cacti
Numéro de Référence	39751201/23
Date de publication	12 Janvier 2023
Risque	Important
Impact	Critique

Systemes affectés

- Cacti, versions antérieures à 1.2.23

Identificateurs externes

- CVE-2022-38023, CVE-2022-37966, CVE-2022-37967, CVE-2022-45141

Bilan de la vulnérabilité

Des chercheurs en sécurité informatique annoncent la découverte d'une vulnérabilité critique affectant le logiciel de surveillance réseau Cacti. L'exploitation de cette vulnérabilité peut permettre à un attaquant distant d'exécuter du code arbitraire.

Solution

Veillez se référer à la page de Cacti su Github afin d'installer les nouvelles mises à jour.

Risque

- Exécution de code arbitraire à distance.

Référence

Rapport de Sonarsource concernant cette vulnérabilité:

- <https://www.sonarsource.com/blog/cacti-unauthenticated-remote-code-execution/>

Page de Cacti sur Github :

- <https://github.com/Cacti/cacti/security/advisories/GHSA-6p93-p743-35gf>