



BULLETIN DE SECURITE

Titre	Vulnérabilités dans l'hyperviseur Xen
Numéro de Référence	39010311/22
Date de Publication	03 Novembre 2022
Risque	Important
Impact	Important

Systemes affectés

- Xen toutes versions sans le dernier correctif de sécurité du 01 Novembre 2022

Identificateurs externes

- CVE-2022-42325 CVE-2022-42326 CVE-2022-42324 CVE-2022-42322 CVE-2022-42323 CVE-2022-42321 CVE-2022-42320 CVE-2022-42319 CVE-2022-42310 CVE-2022-42309 CVE-2022-42327 CVE-2022-42311 CVE-2022-42312 CVE-2022-42313 CVE-2022-42314 CVE-2022-42315 CVE-2022-42316 CVE-2022-42317 CVE-2022-42318

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les versions d'hyperviseur Xen susmentionnées. L'exploitation de ces failles peut permettre à un attaquant de causer un déni de service, de porter atteinte à la confidentialité de données et de réussir une élévation de privilèges.

Solution

Veillez se référer au bulletin de sécurité Xen du 01 Novembre 2022.

Risque

- Déni de service
- Atteinte à la confidentialité de données
- Elévation de privilèges

Annexe

Bulletins de sécurité Xen du 01 Novembre 2022:

- <https://xenbits.xen.org/xsa/advisory-421.html>
- <https://xenbits.xen.org/xsa/advisory-420.html>
- <https://xenbits.xen.org/xsa/advisory-419.html>

- <https://xenbits.xen.org/xsa/advisory-418.html>
- <https://xenbits.xen.org/xsa/advisory-417.html>
- <https://xenbits.xen.org/xsa/advisory-416.html>
- <https://xenbits.xen.org/xsa/advisory-415.html>
- <https://xenbits.xen.org/xsa/advisory-414.html>
- <https://xenbits.xen.org/xsa/advisory-412.html>
- <https://xenbits.xen.org/xsa/advisory-326.html>