



BULLETIN DE SECURITE

| | |
|----------------------------|---|
| Titre | Vulnérabilités dans les processeurs AMD |
| Numéro de Référence | 37301407/22 |
| Date de Publication | 14 Juillet 2022 |
| Risque | Important |
| Impact | Important |

Systemes affectés

- Processeurs AMD Athlon X4
- Processeurs AMD Ryzen Threadripper PRO
- Processeurs AMD Ryzen Threadripper deuxième génération
- Processeurs AMD Ryzen Threadripper troisième génération
- Processeurs AMD Séries A APUs septième génération
- Processeurs AMD Ryzen 2000 Séries Desktop
- Processeurs AMD Ryzen 3000 Séries Desktop
- Processeurs AMD Ryzen 4000 Séries Desktop avec circuit graphique Radeon
- Processeurs AMD Ryzen 2000 Séries Mobile
- Processeurs AMD Athlon 3000 Séries Mobile avec Radeon
- Processeurs AMD Ryzen 3000 Séries Mobile ou AMD Ryzen Mobile seconde génération avec circuit graphique Radeon
- Processeurs AMD Ryzen 4000 Séries Mobile avec circuit graphique Radeon
- Processeurs AMD Ryzen 5000 Séries Mobile avec circuit graphique Radeon
- Processeurs AMD Athlon Mobile avec circuit graphique Radeon
- Processeurs AMD EPYC première génération
- Processeurs AMD EPYC seconde génération

Identificateurs externes

- CVE-2017-5715, CVE-2022-29900, CVE-2022-23825

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les processeurs AMD susmentionnés. Un attaquant distant pourrait exploiter certaines de ces vulnérabilités afin d'exécuter du code arbitraire à distance, accéder aux informations confidentielles ou contourner la politique de sécurité.

Solution :

Veillez se référer aux bulletins de sécurité AMD du 12 Juillet 2022 afin d'installer les nouvelles mises à jour.

Risque :

- Exécution du code arbitraire à distance
- Contournement de la politique de sécurité
- Accès aux informations confidentielles

Référence :

Bulletins de sécurité AMD du 12 Juillet 2022:

- <https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1037>