ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant des produits AMD
Numéro de Référence	39191011/22
Date de publication	10 Novembre 2021
Risque	Important
Impact	Important

Systèmes affectés

- AMD Link Android App
- AMD Radeon™ RX 5000 Series and
- AMD Radeon™ PRO W5000 Series Graphics Cards
- AMD Radeon™ RX 6000 Series and
- AMD Radeon™ PRO W6000 Series Graphics Cards
- AMD Athlon™ X4 processor
- AMD Ryzen™ Threadripper™ PRO processor
- 2nd Gen AMD Ryzen™ Threadripper™ processors
- 3rd Gen AMD Ryzen™ Threadripper™ processors
- 7th Generation AMD A-Series APUs
- AMD Ryzen™ 2000 Series Desktop processors
- AMD Ryzen™ 3000 Series Desktop processors
- AMD Ryzen™ 4000 Series Desktop processors with Radeon™ graphics
- AMD Ryzen™ 2000 Series Mobile processor
- AMD Athlon™ 3000 Series Mobile processors with Radeon™ graphics
- AMD Ryzen™ 3000 Series Mobile processors or 2nd Gen AMD Ryzen™ Mobile processors with Radeon™ graphics
- AMD Ryzen™ 4000 Series Mobile processors with Radeon™ graphics
- AMD Ryzen™ 5000 Series Mobile processors with Radeon™ graphics
- AMD Athlon™ Mobile processors with Radeon™ graphics
- 1st Gen AMD EPYC™ processors
- 2nd Gen AMD EPYC™ processors
- 3rd Gen AMD EPYC™ processors
- AMD µProf

Pour plus d'informations sur les versions affectées veuillez consulter le bulletin de sécurité d'AMD.

Identificateurs externes

CVE-2022-27673	CVE-2022-23824	CVE-2020-12930	CVE-2020-12931
CVE-2021-26391	CVE-2021-26392	CVE-2021-26393	CVE-2021-26360

Bilan de la vulnérabilité

AMD annonce la correction de plusieurs vulnérabilités affectant ses produits susmentionnés. En exploitant ces vulnérabilités, un attaquant peut exécuter du code arbitraire, accéder à des informations confidentielles, élever ses privilèges ou causer un déni de service.

Solution

Veuillez se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs.

Risque

- Exécution de code arbitraire
- Accès à des informations confidentielles
- Elévation de privilèges
- Déni de service

Référence

Bulletins de sécurité d'AMD :

- https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1047
- https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1029
- https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1040
- https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1046