CYBER DEFENSE AFRICA : ANNONCE SÉCURITÉ **Date** : 31/05/2022

Type de Contenu	Description
Titre	*Zero-day dans la suite Office de Microsoft*
ID	*202205/Alerte/04*
Code LTP	*White*
Niveau de Risque	*Élevé*
Application et service Affectés	*Microsoft Office*
Version	*2013, 2016, 2019, 2021 et les versions Professional Plus*
Plateforme	*NA*
Mise à jour	*NA*
Résumé	*Vulnérabilité permettant l'exécution de code arbitraire avec les privilèges de l'application appelante sur les systèmes affectés*
Impacts	*L'attaquant qui réussit à exploiter cette vulnérabilité peut :* - *Installer des programmes* - *Visualiser, modifier ou supprimer des données* - *Créer de nouveaux comptes dans le contexte autorisé par les droits de l'utilisateur.*
Description Détaillée	*La vulnérabilité Zéro-day à laquelle est maintenant attribué l'identifiant CVE-2022-30190, est évaluée à 7,8 sur 10 pour la gravité dans le système de notation des vulnérabilités CVSS.* *Cette vulnérabilité apparait lorsque le MDST (Microsoft Support Diagnostic Tool) est appelé à l'aide du protocole URL à partir d'une application appelante telle que Word.*
Solutions	*Afin de protéger ces clients, Microsoft a publié sur leur site web des conseils à appliquer (cliquer sur le deuxième lien dans **liens pour plus de détails**)*
Liens pour plus de détails	*https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190* *https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/*