CYBER DEFENSE AFRICA : ANNONCE DE SÉCURITÉ **Date** : 05/02/2025

Type de Contenu	Description
Titre	***Vulnérabilités en cours d'exploitation, urgence d'appliquer les patchs disponibles***
ID	*202502/AS/07*
Code TLP	*Green*
Niveau de Risque	***Critique***
Application et service affectés	• *Apache OFBiz,* • *Microsoft.NET Framework,* • *Paessler PRTG Network Monitor*
Version / Edition	• *Apache OFBiz, toutes les versions antérieures à 18.12.16,* • *Microsoft.NET Framework versions 2.0, 3.0, 3.5, 4.6.x, 4.7.x, 4.8 et 4.8.1,* • *PRTG Network Monitor antérieure à la version 18.2.39,* • *PRTG Network Monitor version antérieure à 18.2.40.1683*
Plateforme	***Apache OFBiz,*** ***Windows 10, Windows 11 et Windows Server,*** ***Paessler PRTG Network Monitor***
Mise à jour	• *Apache OFBiz 18.12.17 ou ultérieure,* • *Microsoft.NET Framework ultérieure à 4.8.1,* • *PRTG Network Monitor Version 18.2.40 ou ultérieure*
Résumé	*Quatre (04) vulnérabilités en cours d'exploitation : des mises à jour urgentes sont requises pour se protéger.*
Impacts	***Divulgation des données sensibles, Création et élévation de privilèges des utilisateurs, Prise de contrôle des systèmes, Accès non autorisé aux services et données sensibles.***
Description Détaillée	*Une liste de quatre (04) vulnérabilités viennent d'être formellement identifiées comme étant en cours d'exploitation dans les attaques. Il s'agit de :* • ***CVE-2024-45195*** *(CVSS score 9.8) : est une vulnérabilité de navigation forcée dans Apache OFBiz qui permet à un attaquant distant d'obtenir un accès non autorisé et d'exécuter du code arbitraire sur le serveur (Corrigée en Septembre 2024).* • ***CVE-2024-29059*** *(CVSS score 7.5) : est une vulnérabilité de divulgation d'information dans Microsoft .NET Framework qui pourrait exposer* ***ObjRef URI*** *et conduire à l'exécution de code à distance (corrigée en mars 2024).* • ***CVE-2018-19410*** *(CVSS score : 9.8) : est une vulnérabilité* ***dans Paessler PRTG Network Monitor versions antérieures à 18.2.40.1683*** *qui permet à un attaquant distant non authentifié de créer des utilisateurs avec des privilèges de lecture-écriture (Corrigée en avril 2018).* • ***CVE-2018-9276*** *(CVSS score : 7.2) : concerne une faille qui a été découverte dans* ***PRTG Network Monitor antérieure à la version 18.2.39.*** *Un*

	attaquant ayant accès à la console web PRTG System Administrator avec des privilèges administrateur peut exécuter l'injection de commande OS (à la fois sur le serveur et sur les appareils) en envoyant des paramètres non conformes dans les scénarios de gestion des capteurs ou des notifications (Corrigée en avril 2018). *Toutes ces vulnérabilités ont été corrigées dans les versions ultérieures ou récentes respectifs.*
Recommandations	***Ces vulnérabilités, exploitables dans des attaques, ont toutes été corrigées par les fournisseurs respectifs.*** ***Il est nécessaire d'appliquer urgemment les correctifs afin de se prémunir contre les menaces actives :*** • *CVE-2024-45195 : corrigée dans Apache OFBiz ultérieure à 18.12.16* • *CVE-2024-29059 : corrigée dans Microsoft .NET Framework ultérieurse à 4.8.1* • *CVE-2018-9276 : corrigée dans PRTG Network Monitor version 18.2.39* • *CVE-2018-19410 : corrigée dans PRTG Network Monitor version 18.2.40.1683 ou une version ultérieure*
Indicateurs de Compromission	*NA*
Liens pour plus de détails	*https://ofbiz.apache.org/security.html* *https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29059* *https://www.cve.org/CVERecord?id=CVE-2024-29059* *https://www.cve.org/CVERecord?id=CVE-2018-19410* *https://www.cve.org/CVERecord?id=CVE-2018-9276* *https://www.exploit-db.com/exploits/46527*