ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits IBM
Numéro de Référence	36962006/22
Date de Publication	20 juin 2022
Risque	Important
Impact	Important

Systèmes affectés

- APOGEE PXC Compact (BACnet) versions antérieures à V3.5
- IBM HTTP Server versions 9.0 antérieures à 9.0.5.13
- IBM HTTP Server versions 8.5 antérieures à 8.5.5.23
- IBM HTTP Server versions 8.0 antérieures à 8.0.0.15 sans le correctif PH46897
- IBM HTTP Server versions 7.0 antérieures à 7.0.0.45 sans le correctif PH46897
- IBM Disconnected Log Collector versions 1.x antérieures à 1.7.3
- IBM Analytic Accelerator Framework for Communication Service Providers (AAF) versions 4.0.0.x antérieures à 4.0.0.2
- IBM Customer and Network Analytics for Communications Service Providers and Datasets (CNA) versions 10.0.0.x antérieures à 10.0.0.2
- IBM QRadar SIEM versions 7.3 sans le correctif de sécurité 7.3.0-QRADAR-PROTOCOL-ApacheKafka-7.3-20220429171209
- IBM QRadar SIEM versions 7.4 sans le correctif de sécurité 7.4.0-QRADAR-PROTOCOL-ApacheKafka-7.4-20220429171217
- IBM QRadar SIEM versions 7.5 sans le correctif de sécurité 7.5.0-QRADAR-PROTOCOL-ApacheKafka-7.5-20220429171113
- IBM Rational Test Control Panel component in Rational Test Virtualization Server toutes versions
- IBM Rational Test Control Panel component in Rational Test Workbench toutes versions

Identificateurs externes

- CVE-2021-45046 CVE-2021-44228 CVE-2022-22965 CVE-2020-9547 CVE-2016-8735 CVE-2019-14379 CVE-2020-9548 CVE-2020-9546 CVE-2020-10672 CVE-2020-8840 CVE-2019-14893 CVE-2019-16943 CVE-2019-17531 CVE-2020-10673 CVE-2019-17195 CVE-2019-14540 CVE-2019-14892 CVE-2019-16335 CVE-2019-16942

CVE-2019-20330 CVE-2020-11112 CVE-2020-11113 CVE-2016-0714 CVE-2019-17267 CVE-2020-10968 CVE-2020-10969 CVE-2020-11111 CVE-2021-27568 CVE-2016-5018 CVE-2018-17196

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits IBM susmentionnés. Un attaquant pourrait exploiter ces failles afin d'exécuter du code arbitraire à distance, réussir une élévation de privilèges, causer un déni de service, contourner la politique de sécurité ou porter atteinte à la confidentialité de données.

Solution

Veuillez se référer au bulletin de sécurité IBM du 16 Juin 2022 pour plus d'information.

Risque

- Exécution de code arbitraire à distance
- Elévation de privilèges
- Déni de service
- Contournement de la politique de sécurité
- Atteinte à la confidentialité de données

Annexe

Bulletin de sécurité IBM du 16 Juin 2022 :

- https://www.ibm.com/support/pages/node/6595721
- https://www.ibm.com/support/pages/node/6595755
- https://www.ibm.com/support/pages/node/6595965
- https://www.ibm.com/support/pages/node/6595739

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma