



6 Novembre 2024

URGENT: AVIS DE SÉCURITÉ – IDS-25-5176

Cybersecrurité Produit

REF: voir Tableau 1

Type d'action: action terrain

À l'attention des responsables de laboratoire, des responsables qualité, et des responsables informatiques

Ce courrier contient des informations importantes qui nécessitent votre attention **immédiate**.

Cher client,

BD décide d'une action corrective de sécurité pour les produits listés dans le tableau ci-dessous listant les produits impactés. Selon nos informations, votre établissement/ laboratoire peut avoir une installation d'un ou plusieurs des produits listés dans le tableau ci-dessous.

Nom du Produit	Code Produit (REF)	UDI	SRN Fabricants
BD BACTEC™ Blood Culture System	441385	00382904413859	US-MF-000018910
	445475	00382904454753	
	442296	00382904422967	
BD Phoenix™ M50 Automated Microbiology System	443624	00382904436247	
BD MAX™ System	441916	00382904419165	
BD COR™ System	443988	00382904439880	
	443989	00382904439897	
	443990	00382904439903	
BD EpiCenter™ Microbiology Data Management System	441007	00382904410070	
	440887	00382904408879	
	440981	00382904409814	
BD Synapsys™ Informatics Solution	444150	00382904441500	

Table 1: Produits concernés

Description de l'incident

Grâce à nos outils et processus de surveillance de la cybersécurité, BD a récemment identifié un accès non autorisé à une partie limitée de son environnement technologique de l'information (IT).

BD a mis fin à cet accès non autorisé et a appliqué des mesures de sécurité supplémentaires. Après une enquête approfondie, BD a confirmé que les identifiants de service produit destinés à être utilisés par les équipes de support technique de BD pour certains produits BD ont été accédés par un acteur non autorisé. Jusqu'à ce que ces identifiants de service produit soient mis à jour, il existe un risque d'accès limité non autorisé pouvant affecter la confidentialité, l'intégrité et/ou la disponibilité des produits concernés et du système ou des données associés.

À ce jour, BD n'a pas été informé de l'utilisation non autorisée de ces identifiants de service produit et n'a reçu aucun rapport indiquant que ces identifiants ont été utilisés pour un accès non autorisé à un appareil BD.



Risques cliniques

Un accès non autorisé aux instruments/systèmes BD pourrait être utilisé pour désactiver les instruments, corrompre ou exposer les bases de données des instruments/systèmes ou modifier les résultats des tests diagnostiques. Une désactivation de l'instrument peut retarder un diagnostic et un traitement appropriés. La corruption des données ou la falsification des résultats (où les résultats peuvent être faussement positifs ou faussement négatifs) pourrait entraîner un diagnostic incorrect et un traitement inapproprié ou absent.

À ce jour, il n'y a eu aucune plainte/événement indésirable dans le monde lié à cet événement.

Il n'est pas nécessaire pour le client de retourner à BD les produits énumérés dans le Tableau 1. Ces produits peuvent continuer à être utilisés conformément à la notice.

Ations IT, de sécurité et de sûreté à entreprendre :

BD encourage les clients à poursuivre les meilleures pratiques pour garantir des mesures de sécurité solides afin de protéger les laboratoires hospitaliers et privés, à savoir :

- Assurez-vous que l'accès aux dispositifs potentiellement vulnérables est limité au personnel autorisé.
- Informez les utilisateurs autorisés de l'incident et assurez-vous que tous les mots de passe pertinents sont strictement contrôlés.
- Surveillez et enregistrez le trafic réseau tentant d'atteindre les environnements de gestion des dispositifs médicaux pour détecter toute activité suspecte.
- Lorsque cela est possible, isolez les dispositifs affectés dans un VLAN sécurisé ou derrière des pare-feux avec un accès restreint qui ne permet la communication qu'avec des hôtes de confiance dans d'autres réseaux lorsque cela est nécessaire.
- Désactivez ou bloquez les ports RDP des dispositifs impactés activés, sans nécessité.
- Assurez-vous que les autorisations sur les partages de fichiers sont correctement établies et appliquées, et surveillez et enregistrez l'accès pour détecter toute activité suspecte.
- Déconnectez les dispositifs du réseau si la connectivité n'est pas nécessaire.

Actions de BD :

BD a mis en œuvre des mesures de sécurité supplémentaires pour renforcer de façon significative son environnement IT.

Actions BD en cours :



Les équipes de support régional de BD contacteront les clients en cas d'incident avéré pour les accompagner sur les étapes à suivre, qui peuvent inclure la mise à jour des identifiants et/ou des logiciels.

Actions des clients:

- Examinez les produits listés dans le **tableau 1** pour déterminer si les produits en votre possession sont impactés.
- Complétez et retournez le formulaire de réponse client **même si vous n'utilisez plus/avez plus le produit impacté comme indiqué dans le tableau 1 dans votre établissement avant le 11 décembre 2024.**
- Faites circuler cette notification à tous ceux qui doivent en être informés au sein de votre organisation ou à toute organisation où le produit potentiellement affecté a été transféré.
- Si vous rencontrez des problèmes, veuillez les signaler comme une plainte selon votre processus habituel.

Actions des distributeurs:

- Identifiez les établissements où vous avez distribué le produit affecté et informez-les immédiatement de cette notification.
 - Faites compléter et retourner le formulaire de réponse client à votre organisation à des fins de réconciliation avant le **11 décembre 2024.**
- Complétez et retournez le formulaire de réponse client après avoir terminé vos activités de réconciliation.
- Si vous rencontrez des problèmes, veuillez les signaler comme une plainte selon votre processus habituel.

	Utilisateur final avec stock	Utilisateur sans stock	Où envoyer le formulaire complété
Acheté directement auprès de BD	Complétez le formulaire dans son intégralité et assurez-vous que toutes les actions recommandées ont été mises en œuvre comme requis	Complétez le formulaire dans son intégralité et conservez une copie de cette notification pour vos dossiers	BD_EMEA_Notification@bd.com
Acheté auprès d'un distributeur/tiers	Complétez le formulaire dans son intégralité et assurez-vous que toutes les actions recommandées ont été mises en	Complétez le formulaire dans son intégralité et conservez une copie de cette notification pour vos dossiers	Retournez le formulaire auprès du distributeur/tiers



	œuvre comme requis		
--	-----------------------	--	--

Contact personne de référence

Si vous avez des questions ou avez besoin d'assistance concernant cet avis de sécurité, veuillez contacter votre représentant local BD, ou le bureau local BD, ou envoyer un e-mail à: feedbackinformation.EMEA@bd.com

Nous confirmons que les agences réglementaires appropriées ont été informées de ces actions.

BD s'engage à faire progresser le monde de la santé™. Nos principaux objectifs sont la sécurité des patients et des utilisateurs et vous fournir des produits de qualité. Nous nous excusons pour les désagréments que cette situation pourrait vous causer et vous remercions par avance de votre aide pour résoudre cette affaire aussi rapidement et efficacement que possible.

Cordialement,

Kinga Stolinska
Directrice, Qualité post-marché
Qualité EMEA



Formulaire de réponse client - IDS-25-5176
Problème de cybersécurité des produits REF : Cf Tableau 1

Retournez à BD_EMEA_Notification@bd.com dès que possible ou **au plus tard le 11 décembre 2024**.

En signant ci-dessous, vous confirmez que cet avis de sécurité a été lu, compris et que toutes les actions recommandées ont été mises en œuvre comme requis.

Nom de l'établissement/ laboratoire :	
Département (le cas échéant) :	
Adresse:	
Code Postal:	Pays:
Nom du responsable:	
Titre:	
Numéro téléphone:	E-mail:
Nom de votre fournisseur (si pas acheté directement auprès de BD)*	
Signature:	Date:

Ce formulaire doit être retourné à BD avant que cette action puisse être considérée comme clôturée pour votre compte.

** Si vous avez reçu cet avis de sécurité via un distributeur/tiers, veuillez retourner votre formulaire complété à cette organisation à des fins de réconciliation.*

Veuillez confirmer **UNE** des options suivantes :

- J'ai un ou plusieurs produits affectés au sein de mon organisation.

Veuillez fournir le nom d'un représentant de votre organisation qui sera le point de contact pour organiser la remédiation du produit, si différent de ce qui précède :

<i>Name:</i>	<i>Telephone No:</i>	<i>Email:</i>
--------------	----------------------	---------------

OU

- Je confirme que notre établissement **ne possède aucun** des produits affectés listés dans cet avis de sécurité.

Tous les produits qui ne sont pas disponibles pour la remédiation seront considérés comme disposés à votre emplacement et donc physiquement indisponibles, sauf indication contraire.