28. November 2024

DRINGEND: SICHERHEITSHINWEIS – IDS-25-5176

Produktsicherheit im Bereich Cybersecurity

REF: Siehe Tabelle 1

Art der Aktion: Service Einsatz vor Ort

Achtung: Laborleiter, Risikomanager, IT-Leiter

Dieses Schreiben enthält wichtige Informationen, die Ihre **sofortige** Aufmerksamkeit erfordern.

Sehr geehrter Kunde,

BD führt eine sicherheitsrelevante Korrekturmaßnahme für die in Tabelle 1 aufgeführten Produkte durch. Laut unseren Vertriebsunterlagen könnte Ihre Organisation über eine Installation von einem oder mehreren der in Tabelle 1 genannten Produkte verfügen.

Produktname	Produktcode (REF)	UDI	SN des Herstellers
BD BACTEC™ Blutkultursystem	441385	00382904413859	US-MF-000018910
	445475	00382904454753	
	442296	00382904422967	
	445570	00382904455705	
	445570U	00382904455705	
BD Phoenix™ M50 Automatisiertes Mikrobiologie-System	443624	00382904436247	
BD MAX™ System	441916	00382904419165	
BD COR-System™	443988	00382904439880	
	443989	00382904439897	
	443990	00382904439903	
BD EpiCenter™ Mikrobiologisches Datenmanagementsystem	441007	00382904410070	*N/A*
	440887	00382904408879	
	440981	00382904409814	
BD Synapsys™ Informatics Lösung	444150	00382904441500	

Tabelle 1: Betroffene Produkte

Beschreibung des Problems

Durch unsere Cybersicherheits-Überwachungstools und -prozesse hat BD kürzlich einen unautorisierten Zugriff auf einen begrenzten Teil seiner IT-Umgebung identifiziert. BD hat den unautorisierten Zugriff beendet und zusätzliche Sicherheitsmaßnahmen ergriffen. Nach einer umfassenden Untersuchung bestätigte BD, dass Zugangsdaten für den Produktservice für bestimmte BD-Produkte, die für die Nutzung

durch BD-Techniker vorgesehen sind, von einem unautorisierten Akteur eingesehen wurden. Bis diese Zugangsdaten für den Produktservice aktualisiert werden, besteht das Risiko eines unautorisierten Zugriffs, der die Vertraulichkeit, Integrität und/oder Verfügbarkeit der betroffenen Produkte sowie des zugehörigen Systems oder der Daten beeinträchtigen könnte.

Bislang wurden BD keine Fälle von unautorisiertem Gebrauch dieser Zugangsdaten für den Produktservice bekannt und es liegen keine Berichte vor, dass diese Zugangsdaten für unautorisierten Zugriff auf BD-Geräte genutzt wurden.

Klinisches Risiko

Ein unautorisierter Zugriff auf BD-Instrumente/Systeme könnte genutzt werden, um Instrumente zu deaktivieren, Datenbanken von Instrumenten/Systemen zu beschädigen oder offenzulegen oder diagnostische Testergebnisse zu manipulieren. Eine Deaktivierung von Instrumenten kann eine angemessene Diagnose und Behandlung verzögern. Datenkorruption oder Manipulation von Ergebnissen (wobei Ergebnisse möglicherweise falsch-positiv oder falsch-negativ sein können) könnte zu einer falschen Diagnose und einer unangemessenen oder fehlenden Behandlung führen.

Bis heute sind weltweit keine Beschwerden oder unerwünschten Ereignisse im Zusammenhang mit diesem Vorfall bekannt.

Es ist nicht erforderlich, dass Kunden, die in Tabelle 1 aufgeführten Produkte an BD zurücksenden. Diese Produkte können weiterhin gemäß den Anweisungen in dieser Mitteilung verwendet werden.

IT-, Sicherheits- und Schutzmaßnahmen, die ergriffen werden müssen:

BD empfiehlt Kunden, bewährte Verfahren zur Aufrechterhaltung starker Sicherheitsmaßnahmen zu befolgen, um Krankenhausnetzwerke und medizinische Geräte zu schützen, einschließlich:

- **Sicherstellen**, dass der Zugriff auf potenziell verwundbare Geräte auf autorisiertes Personal beschränkt ist.
- **Autorisierten Benutzern das Problem mitteilen** und sicherstellen, dass alle relevanten Passwörter streng kontrolliert werden.
- **Netzwerkverkehr überwachen und protokollieren**, der versucht, auf die Verwaltungsumgebungen der medizinischen Geräte zuzugreifen, um verdächtige Aktivitäten zu erkennen.
- **Betroffene Geräte nach Möglichkeit isolieren** in einem sicheren VLAN oder hinter Firewalls mit eingeschränktem Zugriff, die nur bei Bedarf die Kommunikation mit vertrauenswürdigen Hosts in anderen Netzwerken erlauben.
- **RDP-Ports deaktivieren oder blockieren**, da betroffene Geräte deren Nutzung nicht erfordern.
- **Berechtigungen auf Dateifreigaben angemessen festlegen und durchsetzen** sowie den Zugriff überwachen und protokollieren, um Hinweise auf verdächtige Aktivitäten zu erhalten.
- **Geräte vom Netzwerk trennen**, wenn eine Konnektivität nicht erforderlich ist.

BD-Maßnahmen:
BD hat zusätzliche Sicherheitsmaßnahmen implementiert, um seine IT-Umgebung weiter zu stärken.

Von BD zu ergreifende Maßnahmen:
Die regionalen Support-Teams von BD werden daran arbeiten, betroffene Kunden zu kontaktieren, um die nächsten Schritte zu besprechen, die möglicherweise die Aktualisierung von Zugangsdaten und/oder Software umfassen.

Vom Kunden zu ergreifende Maßnahmen:

- **Überprüfen Sie die in Tabelle 1 aufgeführten Produkte**, um festzustellen, ob die sich in Ihrem Besitz befindlichen Produkte betroffen sind.
- **Füllen Sie das Kundenantwortformular aus und senden Sie es bis spätestens 11. Dezember 2024 zurück**, auch wenn Sie das betroffene Produkt, wie in Tabelle 1 in Ihrer Einrichtung aufgeführt, nicht mehr verwenden oder besitzen.
- **Verteilen Sie diese Benachrichtigung an alle Personen**, die innerhalb Ihrer Organisation informiert werden müssen, oder an jede Organisation, an die das potenziell betroffene Produkt übertragen wurde.
- **Melden Sie etwaige Probleme als Beschwerde** gemäß Ihrem üblichen Verfahren.

Von Vertriebspartnern zu ergreifende Maßnahmen:

- **Identifizieren Sie die Einrichtungen**, an die Sie das betroffene Produkt verteilt haben, und benachrichtigen Sie diese umgehend über diese Mitteilung.
    - Lassen Sie Ihre Kunden das Kundenantwortformular ausfüllen und für Abgleichzwecke bis zum **11. Dezember 2024** an Ihre Organisation zurücksenden.
- **Füllen Sie das Kundenantwortformular aus und senden Sie es zurück**, nachdem Sie Ihre Abgleichaktivitäten abgeschlossen haben.
- **Melden Sie etwaige Probleme als Beschwerde** gemäß Ihrem üblichen Verfahren.

	Endanwender mit Lagerbestand	**Endanwender OHNE Lagerbestand**	**Wohin ist das ausgefüllte Formular zu senden:**
Direkt von BD gekauft	Das Formular vollständig ausfüllen und sicherstellen, dass alle empfohlenen Maßnahmen wie erforderlich umgesetzt wurden.	Das Formular vollständig ausfüllen und eine Kopie dieser Benachrichtigung für Ihre Unterlagen aufbewahren.	BD_EMEA_Notification@bd.com
Von einem **Vertriebspartner / Drittpartei** gekauft	Das Formular vollständig ausfüllen und sicherstellen, dass alle empfohlenen Maßnahmen wie erforderlich umgesetzt wurden.	Das Formular vollständig ausfüllen und eine Kopie dieser Benachrichtigung für Ihre Unterlagen aufbewahren.	Formular an Ihren Distributor/Drittpartei zurücksenden.

Ansprechpartner

Falls Sie Fragen haben oder Unterstützung in Bezug auf diese Feldsicherheitsmitteilung benötigen, wenden Sie sich bitte an Ihren lokalen BD-Vertreter oder das lokale BD-Büro oder per E-Mail an: feedbackinformation_EMEA@bd.com
Wir bestätigen, dass die entsprechenden Regulierungsbehörden über diese Maßnahmen informiert wurden.

BD hat sich den *Fortschritt für die Welt der Gesundheit*™ zum Ziel gesetzt. Unsere Hauptziele sind die Patientensicherheit und die Sicherheit der Benutzer sowie die Bereitstellung von Qualitätsprodukten. Wir entschuldigen uns für die Unannehmlichkeiten, die diese Situation für Sie verursachen kann, und danken Ihnen im Voraus dafür, dass Sie BD dabei helfen, dieses Problem so schnell und effektiv wie möglich zu lösen.

Mit freundlichen Grüßen,

[redacted]
Direktor, Post-Market-Qualität
EMEA-Qualität

Kundenantwortformular - IDS-25-5176
Produktbezogenes Cybersecurity-Thema
REF: siehe Tabelle 1

Bitte senden Sie das Formular **so schnell wie möglich** oder **spätestens bis zum 11. Dezember 2024 an** BD_EMEA_Notification@bd.com **zurück.**

Mit Ihrer Unterschrift bestätigen Sie, dass Sie diese Feldsicherheitsmitteilung gelesen und verstanden haben und dass alle empfohlenen Maßnahmen wie erforderlich umgesetzt wurden.

Name der Einrichtung:	
Abteilung *(falls zutreffend)*:	
Addresse:	
PLZ:	**Ort:**
Ansprechpartner:	
Funktion/Aufgabenbereich:	
Telefon:	**E-Mail Adresse:**
Name des Lieferanten für Ihr Produkt *(falls nicht direkt über BD erworben)**	
Unterschrift:	**Datum:**

Dieses Formular muss an BD zurückgesendet werden, bevor diese Maßnahme für Ihre Einrichtung als abgeschlossen betrachtet werden kann.

**Wenn Ihnen diese Sicherheitsmitteilung über einen Distributor oder eine dritte Partei weitergeleitet wurde, senden Sie das ausgefüllte Formular bitte an diese Organisation zwecks Abgleichs zurück.*

Bitte bestätigen Sie **EINE** der folgenden Optionen:

☐ Ich habe eines oder mehrere betroffene Produkte in unserer Einrichtung.
Bitte geben Sie den Namen eines Vertreters Ihrer Einrichtung an, der als Ansprechpartner zur Organisation der Produktbehebung zur Verfügung steht, falls dieser von obigen Angaben abweicht:

Name:	*Telefon:*	*Email:*

ODER

☐ Ich bestätige, dass unsere Einrichtung **KEINES** der in dieser Feldsicherheitsmitteilung aufgeführten betroffenen Produkte besitzt.

Alle Produkte, die nicht für eine Nachbesserung verfügbar sind, werden an Ihrem Standort als nicht in Verwendung/ausgemustert betrachtet und sind somit physisch nicht zugänglich, sofern nicht anders angegeben.