

30 september 2025

**BIJGEWERKT**  
**DRINGEND: VEILIGHEIDSKENNISGEVING IN HET**  
**VELD - IDS-25-5176-B**  
**Cyberbeveiliging van producten**  
**REF: Zie Tabel 1**  
**Soort actie: Veldwerk**

**Attentie: laboratoriummanagers, risicomangers, IT-managers**

Deze brief bevat belangrijke informatie die uw **onmiddellijke** aandacht vereist.

Geachte klant,

In november 2024 heeft BD een Field Safety Corrective Action uitgegeven voor een cyberbeveiligingsprobleem van een product (vorige FSN-referentie IDS-25-5176), deze bijgewerkte brief dient als aanvulling op de oorspronkelijke communicatie over veldacties. Het is bedoeld om te verduidelijken dat de eerder beschreven kwestie ongewijzigd blijft; het toepassingsgebied van de betrokken productcodes (REF) is echter uitgebreid.

Deze update documenteert specifiek aanvullende productcodes (REF), waaronder opgeknapte productcodes, die niet in de oorspronkelijke communicatie waren opgenomen.

Dit is geen nieuw probleem, maar een uitbreiding van de oorspronkelijke kennisgeving om ervoor te zorgen dat alle relevante product-ID's volledig worden gedekt.

Volgens onze distributiegegevens kan uw organisatie een installatie hebben van een of meer van de uitgebreide producten die in tabel 1 worden vermeld.

Productnaam	Productcode (REF)	UDI	SRN van de fabrikant
BD EpiCenter™ Microbiologie Gegevens Management Systeem	441002	00382904410025	N.V.T
	441421	00382904414214	
	445398	00382904453985	
	443971	00382904439712	
BD BACTEC™ Bloedkweek Systeem	44138509	00382904413859	US-MF-000018910
	441676	00382904416768	
	44229609	00382904422967	
BD MAX-systeem™	44191609	00382904419165	
Phoenix M50 Instrument	44362409	00382904436247	

**Tabel 1: Beïnvloed product**

**Beschrijving van het probleem**

Via onze tools en processen voor het monitoren van cyberbeveiliging heeft BD onlangs ongeautoriseerde toegang tot een beperkt deel van zijn informatietechnologie (IT)-omgeving geïdentificeerd. BD beëindigde de ongeoorloofde toegang en paste aanvullende beveiligingsmaatregelen toe. Na een grondig onderzoek bevestigde BD dat de inloggegevens voor productservices die bedoeld waren voor gebruik door technische

ondersteuningsteams van BD voor bepaalde BD-producten, toegankelijk waren voor een onbevoegde actor. Totdat deze productservicegegevens zijn bijgewerkt, bestaat er een risico op ongeoorloofde toegang die van invloed kan zijn op de vertrouwelijkheid, integriteit en/of beschikbaarheid van de relevante producten en het bijbehorende systeem of de bijbehorende gegevens.

De producten van BD Diagnostic Solutions die in de klantenbrief worden vermeld, zijn alleen **kwetsbaar als een bedreigingsactor zich fysiek bij het apparaat bevindt en/of het lokale netwerk van uw ziekenhuis of laboratorium heeft geschonden**.

Tot op heden is BD niet op de hoogte gebracht van ongeautoriseerd gebruik van deze productservicegegevens en heeft het geen meldingen ontvangen van het gebruik van deze inloggegevens voor ongeoorloofde toegang tot BD-apparaten.

### **Klinisch risico**

Ongeoorloofde toegang tot BD-instrumenten/-systemen kan worden gebruikt om instrumenten uit te schakelen, instrument-/systeemdatabases te beschadigen of bloot te leggen of diagnostische testresultaten te wijzigen. Een uitschakeling van het instrument kan de juiste diagnose en behandeling vertragen. Gegevensbeschadiging of manipulatie van resultaten (waarbij de resultaten vals-positief of vals-negatief kunnen zijn) kan leiden tot een onjuiste diagnose en ongepaste of afwezige behandeling.

Tot op heden zijn er wereldwijd geen klachten/bijwerkingen geweest die verband houden met dit voorval.

**Klanten zijn niet verplicht om producten zoals vermeld in tabel 1 terug te sturen naar BD. Deze producten kunnen nog steeds worden gebruikt in overeenstemming met de richtlijnen**

### **IT-, veiligheids- en beveiligingsmaatregelen die moeten worden genomen:**

BD moedigt klanten aan om best practices te volgen voor het handhaven van sterke beveiligingsmaatregelen om ziekenhuisnetwerken en medische apparaten te beschermen, waaronder:

- Zorg ervoor dat de toegang tot mogelijk kwetsbare apparaten beperkt is tot geautoriseerd personeel.
- Informeer geautoriseerde gebruikers over het probleem en zorg ervoor dat alle relevante wachtwoorden streng worden gecontroleerd.
- Bewaak en registreer netwerkverkeer dat probeert omgevingen voor het beheer van medische apparaten te bereiken voor Verdachte activiteit.
- Isoleer waar mogelijk getroffen apparaten in een beveiligd VLAN of achter firewalls met beperkte toegang die alleen communicatie met vertrouwde hosts in andere netwerken toestaat wanneer dat nodig is.
- Getroffen apparaten vereisen geen gebruik van RDP-poorten en deze moeten worden uitgeschakeld of geblokkeerd als Ingeschakeld.

- Ervoor zorgen dat machtigingen voor bestandsshares op de juiste manier worden vastgesteld en gehandhaafd, en controleren en Log toegang voor bewijs van verdachte activiteiten.
- Koppel apparaten los van het netwerk als er geen verbinding nodig is.

### **BD-acties:**

BD heeft aanvullende beveiligingsmaatregelen geïmplementeerd om zijn IT-omgeving verder te versterken.

### **Acties die BD moet ondernemen:**

De regionale ondersteuningsteams van BD zullen contact opnemen met de getroffen klanten om de volgende stappen te bespreken, waaronder het bijwerken van inloggegevens en/of software.

### **Acties van de klant:**

- Bekijk de producten in **tabel 1** om te bepalen of de producten in uw bezit zijn Beïnvloed.
- Vul het klantantwoordformulier in en stuur het terug, **zelfs als u het getroffen product zoals vermeld in tabel 1 niet langer in uw faciliteit gebruikt of heeft op 21 oktober 2025.**
- Verspreid deze kennisgeving aan iedereen die op de hoogte moet zijn binnen uw organisatie of aan iedereen die op de hoogte moet zijn organisatie waar het mogelijk getroffen product is overgedragen.
- Als u problemen ondervindt, kunt u dit melden als een klacht volgens uw normale procedure.

### **Acties van distributeurs:**

- Identificeer de faciliteiten waar u het betrokken product hebt gedistribueerd en breng hen onmiddellijk op de hoogte van deze kennisgeving.
  - Laat uw klanten het Customer Response-formulier invullen en terugsturen naar uw organisatie voor afstemmingsdoeleinden vóór **21 oktober 2025.**
- Vul het klantantwoordformulier in en stuur het terug na voltooiing van uw afstemmingsactiviteiten.
- Als u problemen ondervindt, kunt u dit melden als een klacht volgens uw normale procedure.

	<b>Eindgebruiker met voorraad</b>	<b>Eindgebruiker met NUL voorraad</b>	<b>Waar kunt u het ingevulde formulier naartoe sturen?</b>
Rechtstreeks gekocht bij BD	Vul het formulier in zijn geheel in en zorg ervoor dat alle aanbevolen acties zijn geïmplementeerd zoals vereist	Vul het formulier in zijn geheel in en bewaar een kopie van deze kennisgeving voor uw administratie	
Gekocht bij een distributeur/3e partij	Vul het formulier in zijn geheel in en zorg ervoor dat alle aanbevolen acties zijn geïmplementeerd zoals vereist	Vul het formulier in zijn geheel in en bewaar een kopie van deze kennisgeving voor uw administratie	Stuur het formulier terug naar uw distributeur/3e partij



### Contactpersoon

Als u vragen hebt of hulp nodig heeft met betrekking tot deze Field Safety Notice, neem dan contact op met uw lokale BD-vertegenwoordiger of het lokale BD-kantoor of stuur een e-mail naar:

[Redacted]

We bevestigen dat de bevoegde regelgevende instanties op de hoogte zijn gebracht van deze acties.

BD zet zich in om *de wereld van de gezondheidszorg™ vooruit te helpen*. Onze primaire doelstellingen zijn patiëntveiligheid en gebruikersveiligheid en het leveren van kwaliteitsproducten. Wij verontschuldigen ons voor het ongemak dat deze situatie voor u kan veroorzaken en danken u bij voorbaat voor uw hulp aan BD om deze kwestie zo snel en effectief mogelijk op te lossen.

Oprecht

[Redacted]

EMEA-kwaliteit

---

**BIJGEWERKT****Antwoordformulier voor klanten - IDS-25-5176-B  
Cyberbeveiliging van producten is belangrijk  
REF: Zie Tabel 1**

---

Keer zo snel mogelijk of uiterlijk op de **21 oktober 2025 terug naar** [REDACTED].

Door hieronder te ondertekenen, bevestigt u dat deze Field Safety-kennisgeving is gelezen en begrepen en dat alle aanbevolen acties zijn geïmplementeerd zoals vereist.

<b>Naam account/organisatie:</b>	
<b>Afdeling (indien van toepassing):</b>	
<b>Adres:</b>	
<b>Postcode:</b>	<b>Stad:</b>
<b>Naam contactpersoon:</b>	
<b>Functie:</b>	
<b>Contact Telefoonnummer:</b>	<b>Contact E-mailadres:</b>
<b>Naam van uw leverancier voor dit product (indien niet rechtstreeks van BD)*</b>	
<b>Handtekening:</b>	<b>Datum:</b>

*Dit formulier moet worden teruggestuurd naar BD voordat deze actie als gesloten voor uw account kan worden beschouwd.*

*\*Als u deze Field Safety Notice via een distributeur/3rd partij hebt ontvangen, stuur dan uw ingevulde formulier terug naar die organisatie voor afstemmingsdoeleinden.*

Bevestig **EEN** van de volgende opties:

- Ik heb een of meer betrokken producten binnen mijn organisatie.

*Geef de naam op van een vertegenwoordiger van uw organisatie die het aanspreekpunt zal zijn om productsanering te organiseren, indien anders dan hierboven:*

<i>Naam:</i>	<i>Telefoonnummer:</i>	<i>E-mail:</i>

**OF**

- Ik bevestig dat onze faciliteit **geen** van de betrokken producten heeft die in deze Field Safety Notice worden vermeld.

***Alle producten die niet beschikbaar zijn voor sanering, worden beschouwd als verwijderd op uw locatie en daarom fysiek niet beschikbaar, tenzij anders aangegeven.***