

Nota bezpieczeństwa

Analizatory ABL800 Basic i ABL800 FLEX - luki w zabezpieczeniach cybernetycznych

Szanowni Państwo

Firma Radiometer zidentyfikowała trzy potencjalne luki w zabezpieczeniach cybernetycznych analizatorów ABL800 Basic i ABL800 FLEX. Proszę przejść do strony MyRadiometer.com, wybrać opcję „ABL800”, a następnie „Dokumentacja dotycząca cyberbezpieczeństwa”.

Osoba atakująca mająca fizyczny dostęp do analizatora może ominąć tryb kiosku analizatora i uruchomić Menedżera zadań systemu Windows.

Wykorzystując wszystkie trzy luki jednocześnie, osoba atakująca może uzyskać zdalną kontrolę nad analizatorem, jeśli działa on w systemie Windows XP lub Windows 7. Uzyskanie zdalnej kontroli nad analizatorami działającymi w systemie Windows 10 nie jest możliwe.

Zdalne sterowanie może być wykorzystane na przykład do uniemożliwienia korzystania z analizatora lub jako punkt ataku na sieć, do której analizator jest podłączony. Atakujący będzie mógł przeglądać dane pacjentów i wyniki pomiarów, ale nie będzie mógł zmieniać zaszyfrowanych danych, dlatego luki w zabezpieczeniach nie doprowadzą do niebezpiecznej sytuacji.

Wpływ na bezpieczeństwo pacjentów

Nie ma to wpływu na bezpieczeństwo pacjentów.

Produkty, których dotyczy problem

Analizatory ABL800 Basic i ABL800 FLEX w następujących konfiguracjach:

- Windows XP i wszystkie wersje oprogramowania aplikacyjnego
- Windows 7 i wszystkie wersje oprogramowania aplikacyjnego
- Windows 10 i oprogramowanie aplikacyjne w wersji niższej niż SW 6.20 MR2

ABL800 Basic: 57006900036MW

ABL8xx FLEX: 57006900037MY

(UDI = Unique Device Identifier – DI = Device Identifier)

Co należy zrobić

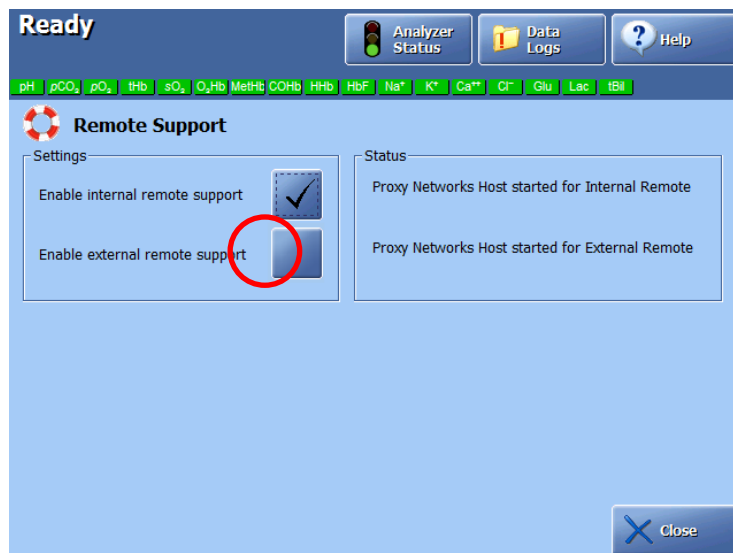
Aby móc dalej korzystać z analizatora, firma Radiometer prosi o upewnienie się, że:

1. Dostęp do analizatora mają tylko upoważnione osoby.
2. Sieć jest bezpieczna, a dostęp do niej odbywa się zgodnie z najlepszymi praktykami.

Jeśli wymagania dotyczące sieci nie są spełnione, firma Radiometer uprzejmie prosi o:

- W przypadku analizatorów z systemem Windows XP:

Wyłączenie zewnętrznego dostępu zdalnego do analizatora(-ów) poprzez usunięcie zaznaczenia opcji „Włącz zewnętrzne wsparcie zdalne”, jeśli jest zaznaczona, jak pokazano na poniższym zrzucie ekranu.



- W przypadku analizatorów z systemem Windows 7:
 - Jeśli oprogramowanie analizatora ma wersję niższą niż 6.20 MR2, należy fizycznie odłączyć analizator od sieci, odłączając kabel.
 - Jeśli oprogramowanie analizatora ma wersję 6.20 MR2, nie są wymagane żadne dodatkowe działania ze strony użytkownika
- W przypadku analizatorów z systemem Windows 10:

Nie są wymagane żadne dodatkowe działania ze strony użytkownika, ponieważ osoba atakująca nie może uzyskać zdalnej kontroli nad tymi analizatorami.

Dodatkowo prosimy o wypełnienie formularza odpowiedzi zwrotnej (dołączonego do niniejszego pisma) i odesłanie go do przedstawiciela firmy Radiometer w ciągu dwóch tygodni od otrzymania niniejszego pisma (*Formularz prosimy odesłać na adres e-mail: incydenty@radiometer.pl lub do siedziby firmy na adres: Radiometer Sp. z o.o., Al. Jerozolimskie 181A, 02-222 Warszawa*).

Rozwiązanie zapewnione przez firmę Radiometer

Lokalny przedstawiciel firmy Radiometer skontaktuje się z Państwem w celu wyjaśnienia trwałego rozwiązania i umówienia wizyty w celu wdrożenia go w analizatorze.

Będziemy wdzięczni za pomoc

Jeśli cyberbezpieczeństwo nie należy do zakresu Państwa obowiązków, prosimy o przekazanie niniejszej informacji zespołowi IT.

W razie jakichkolwiek pytań prosimy o kontakt z przedstawicielem firmy Radiometer.

Firma Radiometer szczerze przeprasza za niedogodności, jakie może spowodować ta sytuacja.

Z poważaniem,

Radiometer Sp. z o.o.
AL. Jerozolimskie 181A
02-222 Warszawa

Formularz odpowiedzi zwrotnej

Dotyczy:

Luki w zabezpieczeniach cybernetycznych

☐ Otrzymałem pismo informacyjne dla klientów i potwierdzam, że:

☐ Tylko upoważnione osoby mają fizyczny dostęp do analizatora.

Ponadto:

☐ Nie mam żadnych analizatorów podłączonych do sieci.

Lub

☐ Mam analizatory podłączone do sieci i mogę potwierdzić, że:

☐ Sieć jest bezpieczna, a dostęp do niej odbywa się zgodnie z najlepszymi praktykami.

Lub

☐ Wymagania sieciowe nie są spełnione, a działania wymagane dla różnych kombinacji analizatorów, wersji systemu Windows i wersji oprogramowania aplikacyjnego zostały wykonane.

Nazwa Szpitala:	
Imię i nazwisko:	
Data:	
Podpis:	
Email:	