Biuletyn Obsługi technicznej
Okno dialogowe Windows Security
Numer kontrolny D000185325/B

Numer Biuletynu Obsługi technicznej: D000185325

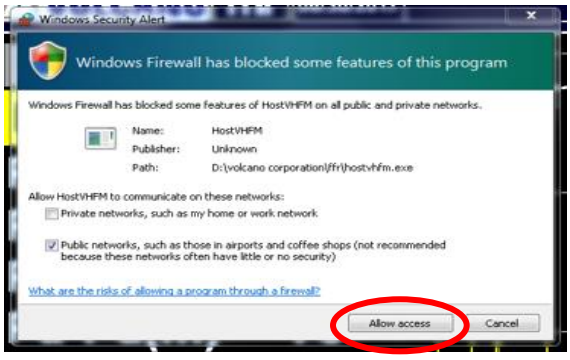
Data wydania: 21.11.2017 r. **Dokument wchodzi w życie z dniem: 21.11.2017 r.**

Temat: Okno dialogowe Windows Security

Produkty, których dotyczy biuletyn:
Systemy s5i/CORE/CORE Mobile z wersją oprogramowania v3.5 („Systemy Zagrożone Usterką").

Cel komunikacji:
Powiadomienie klientów o problemie z oknem dialogowym Windows Security dotyczącym Systemów Zagrożonych Usterką i komunikacji sieci szpitalnej oraz przekazanie im sposobów postępowania, które pozwolą zapobiegać występowaniu usterki związanej z oknem dialogowym Windows Security.

Podsumowanie usterki technicznej:
Volcano Corporation uzyskało wiedzę, że ustawienia bezpieczeństwa Microsoft Windows zostały niepoprawnie skonfigurowane podczas produkcji niewielkiej ilości Systemów Zagrożonych Usterką. Ta niepoprawna konfiguracja może prowadzić do pojawienia się okna dialogowego Windows Security, gdy system przełącza się z trybu IVUS na tryb FFR/iFR (Cząstkowa rezerwa przepływu wieńcowego/Przezzwężeniowy gradient ciśnień w fazie rozkurczowej cyklu pracy serca). Jeśli użytkownik udzieli w oknie dialogowym odpowiedzi „Allow access" („Zezwól na dostęp") (jak pokazano poniżej), ustawienia sieciowej zapory firewall urządzenia zostaną zmodyfikowane, co poskutkuje otwarciem portów sieciowych urządzenia na potencjalną nieoczekiwaną komunikację z sieci szpitalnej, z którą urządzenie może być połączone.



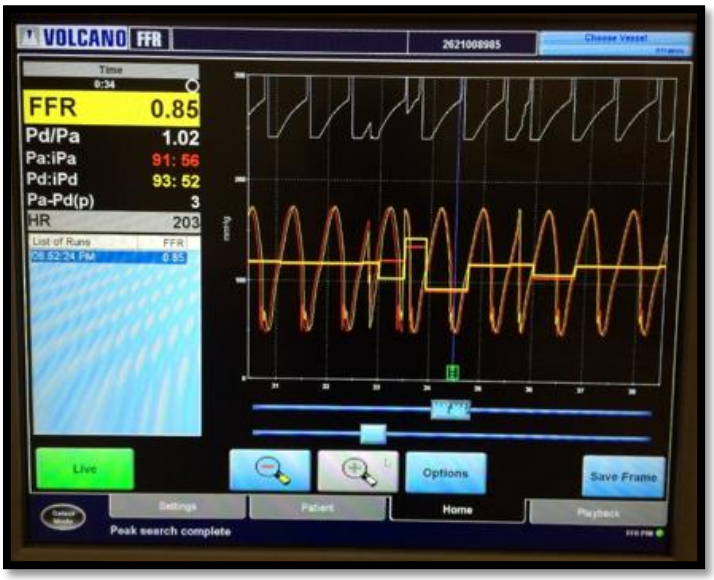
Rysunek 1 – Okno dialogowe Windows Security

Jeżeli zostanie wybrana opcja „Allow access" („Zezwól na dostęp"), a System Zagrożony Usterką odbierze nieoczekiwaną komunikację z sieci szpitalnej podczas przeprowadzania procedury FFR/iFR, może to mieć wpływ na zapis danych, co z kolei może prowadzić do potencjalnej utraty danych, która może zakłócać pomiary FFR lub iFR dokonywane podczas otrzymania nieoczekiwanej komunikacji.

Jeżeli System Zagrożony Usterką odbierze nieoczekiwaną komunikację z sieci szpitalnej, mogą mieć miejsce następujące scenariusze:

Scenariusz 1
Systemy Zagrożone Usterką: oprogramowanie wersji v3.5 działające na systemie s5i/CORE/CORE Mobile po wybraniu opcji „Allow access" („Zezwól na dostęp") w oknie dialogowym Windows Security

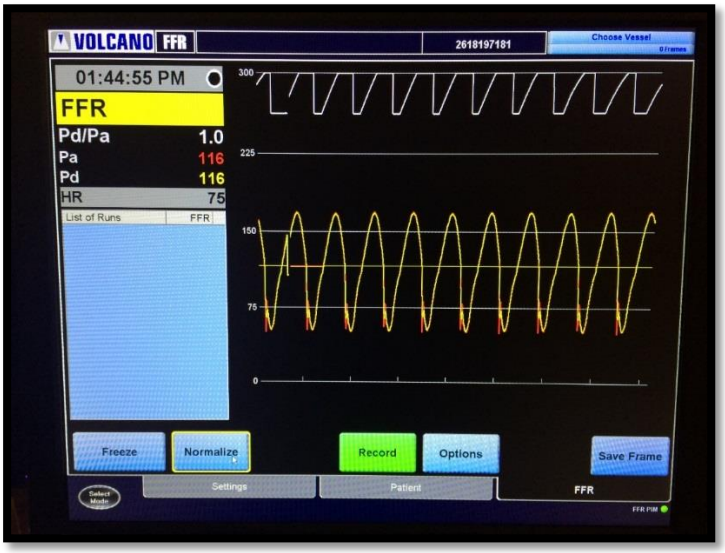
Gdy System Zagrożony Usterką odbierze nieoczekiwaną komunikację podczas pracy w trybie FFR/iFR lub RECORD (Rejestracja), proces odświeżania krzywych ciśnień oraz ECG może zostać na chwilę wstrzymane, a krzywe zostaną zniekształcone (zobacz **Rysunek 2**). Zapisy uzyskane podczas pomiaru, w którym wystąpiła taka usterka nie powinny być używane.



Rysunek 2: Zrzut ekranu FFR w momencie, gdy System Zagrożony Usterką odbiera nieoczekiwaną komunikację z sieci szpitalnej

Scenariusz 2
Systemy Zagrożone Usterką: oprogramowanie wersji v3.5 działające na systemie s5i/CORE/CORE Mobile po wybraniu opcji „Allow access" („Zezwól na dostęp") w oknie dialogowym Windows Security

Gdy System Zagrożony Usterką odbierze nieoczekiwane dane podczas pracy w trybie FFR/iFR lub RECORD, proces odświeżania krzywych ciśnień oraz ECG zostanie zatrzymany. Krzywe przestaną być odświeżane na monitorze **(zobacz RYSUNEK 3)**.



Rysunek 3: Zrzut ekranu FFR w momencie utraty krzywych ECG i Ciśnień, gdy System Zagrożony Usterką napotyka nieoczekiwaną komunikację z sieci szpitalnej

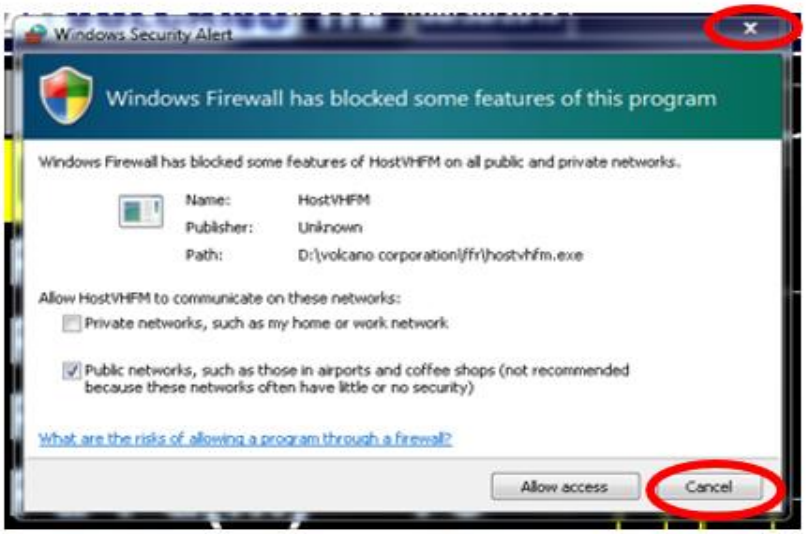
Jeden z powyższych scenariuszy może mieć miejsce wtedy, gdy zostaną spełnione wszystkie poniższe warunki:

- System jest włączony i wykorzystuje oprogramowanie w wersji v3.5
- Jest połączony kablem z siecią szpitalną
- Użytkownik przełącza się z trybu IVUS na tryb FM
- Pojawia się okno dialogowe zapory ogniowej Windows Firewall
- Użytkownik wybiera opcję „Allow access" („Zezwól na dostęp")
- Zaczynają być pobierane dane ciśnień FFR/iFR
- System odbiera nieoczekiwana komunikację od sieci szpitalnej podczas dokonywania pomiaru FFR, iFR

Naprawianie usterki:

Philips Volcano przeprowadzi inspekcję oprogramowania systemów w ramach procesu Konserwacji Profilaktycznej lub Serwisu. Do tego czasu, mogą Państwo kontynuować używanie systemu, pod warunkiem poczynienia poniższych kroków:

1. O ile będzie to możliwe, przed rozpoczęciem pomiaru pacjenta nalezy uruchomić ponownie system i przełączyć urządzenie w tryb FFR/iFR po ponownym uruchomieniu systemu. Jeśli pojawi się okno dialogowe Widnows, należy wybrać opcję „Cancel" („Anuluj"), lub „X" w prawym górnym rogu okna (Rysunek 4).

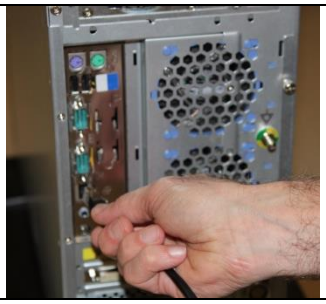


Rysunek 4

2. Jeśli wykonują Państwo procedurę, można także odłączyć System Zagrożony Usterką od sieci szpitalnej. (Rysunek 5)
3. Jeśli w Systemie Zagrożonym Usterką pojawi się okno dialogowe Windows Security, należy skontaktować się z Biurem ds. wsparcia technicznego Philips Volcano, by umówić termin wizyty serwisowej, podczas której usterka zostanie naprawiona.

Wszystkie zmiany dotyczące zezwalania na dostęp w zaporze ogniowej firewall, które zostały wprowadzone przez wybranie opcji „Allow access" („Zezwól na dostęp") będą automatycznie usunięte podczas ponownego uruchomienia systemu. Jednakże, komunikat Windows Security może pojawiać się ponownie po każdym ponownym uruchomieniu systemu.

- **Uwaga:** odłączenie systemu od sieci szpitalnej spowoduje ograniczenie działania funkcjonalności Worklist oraz możliwości archiwizowania danych w sieci PACS w czasie, gdy system pozostaje odłączony od sieci placówki. Jeśli musisz ponownie podłączyć system do sieci w celu zarchiwizowania danych, gdy nie jest używany do przeprowadzania procedury, upewnij się, że zostanie od ponownie odłączony od sieci przed rozpoczęciem procedury.

	
CORE	**CORE Mobile**
	
s5i	**s5**

Rysunek 5: Aby odłączyć Systemy Zagrożone Usterką od sieci placówki, należy odłączyć kabel interfejsu sieciowego od tylnego panelu systemu. Kabel ten może zostać również odłączony po stronie sieci placówki.

Jeśli w Systemie Zagrożonym Usterką pojawi się okno dialogowe Windows Security, należy skontaktować się z Biurem ds. wsparcia technicznego Philips, by umówić termin wizyty serwisowej, podczas której usterka zostanie trwale naprawiona.

Pozostałe uwagi:

Użytkownik może zignorować okno dialogowe Windows Security przemieszczając je w inne miejsce na monitorze i kontynuując procedurę. Jest to dopuszczalne rozwiązanie, które nie będzie miało wpływu na bezpieczeństwo systemu oraz pozyskiwanie danych FFR/iFR.

Zmiany dotyczące zezwalania na dostęp w zaporze ogniowej firewall będą automatycznie usunięte podczas ponownego uruchomienia systemu, jednak komunikat Windows Security będzie pojawiał się nadal po każdym ponownym uruchomieniu. Należy skontaktować się z Biurem ds. Pomocy technicznej, by na stałe wyeliminować tę usterkę.

Kontakt z Volcano:
Jeśli potrzebujecie Państwo dodatkowych informacji, należy skontaktować się z:

Volcano Corporation
2870 Kilgore Road
Rancho Cordova, CA 95670
Stany Zjednoczone
(800) 228-4728 Opcja (2)
916-358-8492 FAX

Volcano International
Technical support
Department
Excelsiorlaan 41
1930 Zaventem
Belgium
Tel: 00 32 2 713 18 20
techsupporteu@philips.com