<u>Pilna informacja dotycząca bezpieczeństwa</u>

Wykonywanie aktualizacji systemów Antywirusowych i Windows na serwerach iQ-WEBX.

Dotyczy iQ-X 2.2.0 (z ważną licencją na oprogramowanie)

---

6 listopada 2017 r.

Nadawca:

IMAGE Information Systems Europe GmbH
Dr Arpad Bischof
Safety Officer for Medical Devices
Lange Str. 16
18055 Rostock
Niemcy

Adresat:

Niniejsze informacje dotyczące bezpieczeństwa są przeznaczone dla następujących grup docelowych:

- Wszyscy operatorzy instalacji iQ-WEBX z oprogramowaniem iQ-X 2.2.0 z ważną licencją.
- Wszyscy dystrybutorzy, którzy dystrybuują rozwiązania iQ-WEBX zawierające oprogramowanie iQ-X 2.2.0.

Identyfikacja dotkniętych wyrobów medycznych:

Poniższe wyroby medyczne mogą ulec uszkodzeniu:

- iQ-X 2.2.0 (z ważną licencją na oprogramowanie)
- iQ-WEB ≤ 6.4.5 (tylko w połączeniu z licencjonowanym iQ-X 2.2.0)
- iQ-4VIEW ≤ 2.0 (tylko w połączeniu z licencjonowanym iQ-X 2.2.0)

Opis problemu, w tym zidentyfikowanej przyczyny:

Począwszy od 37 tygodnia kalendarzowego 2017r. (11-17 Września), niektórzy dostawcy systemów antywirusowych, tacy jak Microsoft, Kaspersky i McAfee, wprowadzili definicje wirusów do swoich produktów bezpieczeństwa, które wykrywają jeden z komponentów naszego

rozwiązania iQ-WEBX jako złośliwe oprogramowanie. Nazwy stwierdzonego zagrożenia różnią się w zależności od dostawcy (np. Trojan: Win32/Rundas. B, Artemis lub Trojan. Win32. Llac. lhwj).

Plik ten nosi nazwę "LicGen. exe" i jest częścią naszego systemu licencjonowania iQ-X. W wyniku takiego wykrycia plik jest usuwany z miejsca pierwotnej lokalizacji w folderze instalacyjnym iQ-WEBX i poddawany kwarantannie lub nawet usuwany.

Jako producent możemy zapewnić, że wykrycie to jest fałszywie pozytywne. Nasze oprogramowanie będące produktem medycznym w wersji dostępnej do pobrania jest wolne od złośliwego oprogramowania. Przedmiotowa dokumentacja istnieje na rynku od kilku lat. Oprogramowanie to nie jest również w stanie komunikować się z niczym innym, jak tylko z lokalną instalacją iQ-WEBX.

W przypadku braku pliku nie jest już możliwe pomyślne zalogowanie się do interfejsu sieciowego iQ-WEB. Typowym objawem jest to, że strona logowania nie zostanie załadowana i okno przeglądarki pozostanie białe.

Oznacza to że:

- Użytkownicy nie będą mieli dostępu do badań oraz informacji dot. danego pacjenta znajdujących się w różnych tabelach.
- Wyświetlanie lub odczyt obrazów nie będą możliwe przy użyciu iQ-WEB, iQ-X lub iQ-4VIEW, co może poważnie utrudnić lub opóźnić proces diagnostyczny.
- Administratorzy nie będą w stanie zarządzać systemem za pomocą interfejsu sieciowego.

Nie ma to jednak wpływu na komunikację DICOM. iQ-WEB będzie w dalszym ciągu otrzymywać dane i dostarczać badania do innych stacji, takich jak iQ-VIEW/PRO.

Jakie środki ma podjąć adresat?

W celu zapewnienia, że problem nie wystąpi w potencjalnie zagrożonym systemie iQ-WEBX, należy podjąć następujące środki.

<u>Jako operator:</u>

1. Przeprowadzić aktualizację serwera iQ-WEBX. Ta aktualizacja powinna zawierać nie tylko najnowsze definicje wirusów, ale także aktualizacje systemu Windows.
2. Uruchomić ponownie serwer, a następnie wykonać skanowanie antywirusowe.
3. Sprawdzić, czy w programie antywirusowym nie znaleziono zagrożeń.
4. Zalogować się do iQ-WEB i upewnić się, że ma się dostęp do interfejsu sieciowego iQ-X i iQ-4VIEW.

<u>Jako dystrybutor:</u>

1. Skontaktować się z klientami instalacji iQ-WEBX i poprosić ich, aby wykonali wyżej wymienione czynności od 1 do 4 dotyczące potencjalnie zagrożonych systemów.
2. W razie potrzeby wykonać te czynności we współpracy z klientem.

Pomimo podjęcia działań opisanych powyżej istnieje nadal niewielkie prawdopodobieństwo, że dane rozwiązanie antywirusowe wpłynie na poprawne działanie iQ-WEBX. Jeśli nadal nie można zalogować się do interfejsu sieciowego iQ-WEB, mimo że wszystkie usługi na serwerze działają prawidłowo, to może oznaczać to taką właśnie sytuację.

Jeśli tak się stanie, w celu rozwiązania problemu należy postąpić zgodnie z poniższymi instrukcjami:

1. Na serwerze przejść do katalogu instalacyjnego iQ-WEBX, zazwyczaj C:"Program Files"iQ-WEBX.
2. Otworzyć podkatalog "PACS", a następnie "php".
3. Wyszukać plik "LicGen. exe". Powinien znajdować się bezpośrednio w tym folderze, a nie w innym podkatalogu.
4. Jeśli pliku nie ma, należy sprawdzić logi rozwiązania antywirusowego na serwerze, aby zweryfikować, czy plik został przeniesiony do kwarantanny, czy być może nawet usunięty.
5. W przypadku opisanym powyżej najpierw należy spróbować zaktualizować definicje wirusów.
6. Następnie należy przenieść plik "LicGen. exe" z folderu kwarantanny z powrotem do katalogu instalacji <iQ-WEBX>""PACS"php" i wykonać skanowanie antywirusowe.
7. Jeśli plik "LicGen. exe" został całkowicie usunięty z systemu, należy go przywrócić.
   - Dla administratorów: Należy skontaktować się z odpowiedzialnym lokalnym dystrybutorem lub bezpośrednio z producentem pod adresem support@image-systems.biz w celu uzyskania kopii pliku. Należy podać pełny numer wersji.
   - Dla dystrybutorów: Jeśli zainstalowana jest wersja iQ-X 2.2.0.0.6, można pobrać właściwy plik z Sales Partner Login Area tutaj (po uprzednim zalogowaniu się). Jeśli problem dotyczy wcześniejszej wersji iQ-X 2.2.0, skontaktuj się z producentem pod adresem support@image-systems.biz.
8. Plik należy skopiować do folderu instalacji: <Your iQ-WEBX installation directory>\PACS\php\.
9. Podane rozwiązanie powinno zadziałać natychmiast, więc nie jest potrzebny restart serwera lub usługi. Należy zalogować się do iQ-WEB i upewnić się, że jest skuteczny dostęp do interfejsu sieciowego iQ-X i iQ-4VIEW.

Alternatywnie można również dodać plik lub nawet cały folder iQ-WEBX do wyjątków od skanowania. W ten sposób oprogramowanie nie będzie już skanować pliku, nawet jeśli nie będą dostępne żadne nowsze definicje wirusów.

Dalsze działania podjęte ze strony producenta:

Skontaktowaliśmy się z głównymi dostawcami systemów Antywirusowych. Te, które do tej pory odpowiedziały, potwierdziły fałszywie pozytywne wykrywanie i dodały nasz komponent oprogramowania do swoich wykazów. Dlatego też ich najnowsze lub nadchodzące definicje wirusów powinny rozwiązać ten problem.

Ponadto, wprowadzimy zmiany w naszym oprogramowaniu iQ-WEB (dostępnym wraz z kolejną wersją), które usuną zależność pomiędzy komponentem licencji iQ-X a mechanizmem logowania iQ-WEB.

Rozpowszechnianie informacji tu podanych:

Proszę upewnić się w swojej organizacji, że wszyscy użytkownicy wyżej wymienionych produktów oraz wszystkie inne osoby, które powinny zostać poinformowane, są poinformowane o tych pilnych informacjach dotyczących bezpieczeństwa. W przypadku przekazania tych produktów osobom trzecim należy przesłać im kopię tych informacji lub poinformować osobę kontaktową wymienioną poniżej.

Proszę przechowywać te informacje przynajmniej tak długo, jak długo wymienione w nich środki nie zostaną jeszcze całkowicie zakończone.

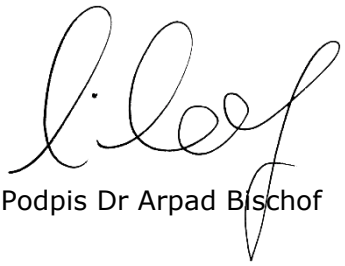
Federalny Instytut Leków i Wyrobów Medycznych w Niemczech otrzymał kopię "Pilnych informacji dotyczących bezpieczeństwa".

Osoba kontaktowa:

Dr Arpad Bischof
Safety Officer for Medical Devices

IMAGE Information Systems Europe GmbH
Lange Str. 16
18055 Rostock
Niemcy

Tel.: +49 381 4 96 58 20
Faks: +49 381 49 65 65 82 99
Tel. kom.: +49 1 57 80 80 26 56 78



Podpis Dr Arpad Bischof