Dringende Sicherheitsinformation

Durchführung von Antivirus- und Windows-Updates auf iQ-WEBX Servern

betreffend

iQ-X 2.2.0 (mit gültiger Softwarelizenz)

---

6. November 2017

Absender:

IMAGE Information Systems Europe GmbH
Dr. Arpad Bischof
Sicherheitsbeauftragter für Medizinprodukte
Lange Straße 16
18055 Rostock
Deutschland

Adressat:

Diese Sicherheitsinformation ist an folgende Zielgruppen gerichtet:

- Alle Betreiber von iQ-WEBX Installationen, welche die Software iQ-X 2.2.0 mit einer gültigen Lizenz beinhalten.
- Alle Händler, die iQ-WEBX Softwarelösungen mit der iQ-X Softwareversion 2.2.0 vertreiben.

Identifikation der betroffenen Medizinprodukte:

Die folgenden Medizinprodukte sind oder könnten betroffen sein:

- iQ-X 2.2.0 (mit gültiger Softwarelizenz)
- iQ-WEB ≤ 6.4.5 (nur bei gleichzeitiger Verwendung eines lizensierten iQ-X 2.2.0)
- iQ-4VIEW ≤ 2.0 (nur bei gleichzeitiger Verwendung eines lizensierten iQ-X 2.2.0)

Beschreibung des Problems einschließlich der ermittelten Ursache:

In Kalenderwoche 37 (11.-17. September 2017) wurden von einigen Antivirus-Herstellern, wie z. B. Microsoft, Kaspersky und McAfee, Virusdefinitionen für deren Sicherheitssoftware veröffentlicht, welche eine der Komponenten unserer iQ-WEBX Softwarelösung als Schadsoftware (also Malware) erkennen. Die Namen dieser gefundenen angeblichen Bedrohung variiert von Anbieter zu Anbieter (z. B. Trojan:Win32/Rundas.B, Artemis oder Trojan.Win32.Llac.lhwj).

Bei der betroffenen Datei handelt es sich um die „LicGen.exe“, welche Teil unseres iQ-X Lizenzsystems ist. Als Folge der Erkennung als Bedrohung wird die Datei aus ihrem Verzeichnis innerhalb des iQ-WEBX Installationsordners entfernt und entweder in die Quarantäne verschoben oder gar vollständig gelöscht.

Wir, als Hersteller, können Ihnen versichern, dass es sich hierbei um eine falsch-positive Erkennung handelt. Unsere Medizinproduktesoftware, so wie sie zum Herunterladen zur Verfügung steht, ist frei von schadhafter Software. Die betroffene Datei befindet sich bereits seit mehreren Jahren auf dem Markt. Sie ist zudem nur darauf ausgelegt, mit der lokalen iQ-WEBX Installation zu kommunizieren. Eine Kommunikation mit anderen Komponenten, Programmen und Systemen ist nicht möglich.

Wenn die Datei fehlt, ist es nicht länger möglich, sich erfolgreich in das iQ-WEB Webinterface einzuloggen. Erkennen tun Sie das daran, dass die Login-Seite nicht geladen wird und das Browserfenster weiß bleibt.

Das bedeutet: Die Anwender haben keinen Zugriff mehr auf die Patienten- und Untersuchungsinformationen, die in den verschiedenen Tabellen von iQ-WEBX präsentiert werden. Das Lesen, Betrachten und Befunden von im Archiv gespeicherten Bilddaten ist weder über iQ-WEB noch über iQ-X oder iQ-4VIEW möglich, was den diagnostischen Arbeitsablauf ernsthaft behindern oder verzögern kann. Administratoren haben zudem nicht mehr die Möglichkeit, das System über die Weboberfläche zu verwalten.

Die DICOM-Kommunikation ist jedoch nicht betroffen. iQ-WEB wird weiterhin Daten empfangen und kann Untersuchungen auch an andere Stationen, wie z. B. iQ-VIEW/PRO, weiterleiten.

Welche Maßnahmen sind durch den Adressaten zu ergreifen?

Die folgenden Maßnahmen sind zu ergreifen, um zu verhindern, dass das Problem auf einem potentiell gefährdeten iQ-WEBX System auftritt.

<u>Als Betreiber:</u>

1. Aktualisieren Sie Ihren iQ-WEBX Server. Das Update sollte nicht nur die neuesten Virusdefinitionen sondern auch die Windows-Updates umfassen.
2. Starten Sie den Server danach neu und führen Sie einen Virenscan durch.
3. Überprüfen Sie die Meldungen des Antivirus-Programms, um herauszufinden, ob irgendwelche Bedrohnungen gefunden wurden.
4. Loggen Sie sich in iQ-WEB ein und stellen Sie sicher, dass Sie auf die Weboberfläche, auf iQ-X und iQ-4VIEW erfolgreich zugreifen können.

Als Händler:

Kontaktieren Sie Ihre Kunden mit iQ-WEBX Installationen und lassen Sie ihren Kunden die oben angeführten Schritte 1 bis 4 auf den gefährdeten Systemen durchführen. Bei Bedarf führen Sie diese Maßnahmen in Abstimmung mit dem Kunden durch.

Trotz der Durchführung der oben angeführten Maßnahmen besteht eine geringe Chance, dass eine bestimmte Antivirus-Lösung iQ-WEBX beeinträchtigt. Sollten Sie feststellen, dass Sie sich nicht länger in die iQ-WEB Weboberfläche einloggen können, obwohl alle Dienste auf dem Server korrekt laufen, dann könnte ein solcher Fall eingetreten sein.

Folgen Sie dann den nachstehenden Anweisungen, um das Problem zu beheben:

1. Navigieren Sie auf dem Server zum iQ-WEBX Installationsverzeichnis, normalerweise unter C:\Programme\iQ-WEBX.
2. Öffnen Sie den Unterordner „PACS“ und dann „php“.
3. Suchen sie nach der Datei „LicGen.exe“. Diese sollte sich direkt in diesem Ordner befinden, nicht in einem anderen Unterordner.
4. Falls die Datei nicht vorhanden sein sollte, überprüfen Sie die Logdateien der Antivirus-Lösung auf dem Server, um herauszufinden, ob die Datei in die Quarantäne verschoben oder vielleicht gelöscht wurde.
5. Sollte das der Fall sein, versuchen Sie zunächst, die Antivirusdefinitionen zu aktualisieren.
6. Verschieben Sie danach die „LicGen.exe“ vom Quarantäne-Ordner zurück nach <iQ-WEBX Installationsverzeichnis>\PACS\php\ und führen Sie einen Virenscan aus.
7. Sollte die „LicGen.exe“ komplett vom System gelöscht worden sein, müssen Sie diese Datei wieder herstellen.
   Für Betreiber: Wenden Sie sich an Ihren zuständigen Händler oder direkt an uns über support@image-systems.biz, um eine Kopie der Datei zu erhalten. Nennen Sie uns dafür die komplette Versionsnummer.
   Für Händler: Haben Sie bzw. Ihre Kunden iQ-X 2.2.0.6 installiert, so können Sie die Datei hier aus unserem Händlerbereich herunterladen. Denken Sie daran, sich dafür zunächst im Händlerbereich einzuloggen. Sollte eine frühere iQ-X 2.2.0 Version betroffen sein, dann kontaktieren Sie uns über support@image-systems.biz.
8. Kopieren Sie die Datei in folgenden Ordner: <Ihr iQ-WEBX Installationsverzeichnis>\PACS\php\.
9. Diese Lösung sollte sofort Abhilfe schaffen; ein Neustart des Systems oder der Dienste ist nicht erforderlich. Loggen Sie sich in iQ-WEB ein und stellen Sie sicher, dass Sie auf die Weboberfläche, auf iQ-X und iQ-4VIEW erfolgreich zugreifen können.

Als Alternative können Sie auch die Datei oder aber den gesamten iQ-WEBX Ordner zu den Scan-Ausnahmen hinzufügen. Auf diese Weise wird die Antivirus-Software die Datei nicht länger scannen, auch falls keine neueren Virusdefinitionen verfügbar sein sollten.

Weitere Maßnahmen von unserer Seite:

Wir haben die Hauptanbieter von Antiviruslösungen kontaktiert. Diejenigen, die auf unsere Anfrage geantwortet haben, bestätigten die falsch-positive Erkennung und haben unsere Softwarekomponente auf ihre Whitelists gesetzt. Ihre aktuellsten bzw. anstehenden Virusdefinitionen sollten den Fehler also korrigieren.

Zusätzlich werden wir mit dem nächsten Release Änderungen an unserer iQ-WEB Software vornehmen, um die Abhängigkeit der iQ-X Lizenzkomponente vom iQ-WEB Login-Mechanismus zu entfernen.

Weitergabe der hier beschriebenen Informationen:

Bitte stellen Sie in Ihrer Organisation sicher, dass alle Anwender der o. g. Produkte und sonstige zu informierende Personen Kenntnis von dieser Dringenden Sicherheitsinformation erhalten. Sofern Sie die Produkte an Dritte abgegeben haben, leiten Sie bitte eine Kopie dieser Information weiter oder informieren Sie die unten angegebene Kontaktperson.

Bitte bewahren Sie diese Information zumindest solange auf, bis die Maßnahme abgeschlossen wurde.

Das Bundesinstitut für Arzneimittel und Medizinprodukte hat eine Kopie dieser „Dringenden Sicherheitsinformation“ erhalten.

Kontaktperson:

Dr. Arpad Bischof
Sicherheitsbeauftragter für Medizinprodukte

IMAGE Information Systems Europe GmbH
Lange Straße 16
18055 Rostock
Deutschland

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