LOWTeq GmbH | Widdersdorfer Straße 236 - 240 | 50825 Köln

Köln den 16.09.2022

Dringende Sicherheitsinformation

Behebung von Sicherheitslücken
betreffend
LOWTeq*pdms*

Absender

LOWTeq GmbH
Abteilung Support
Mail: support@lowteq.de
Tel: +49 221 502946 12

Adressat

IT-Abteilungen der Kunden von LOWTeq

Identifikation der betroffenen Medizinprodukte

Betroffen sind alle Versionen von LOWTeq*pdms* bis zur Version 7.24.02. Höhere Versionen sind nicht betroffen.

Beschreibung des Problems einschließlich der ermittelten Ursache

Im Rahmen eines Security-Tests (auch Penetration-Tests) wurde eine Sicherheitslücke in LOWTeq*pdms* identifiziert. Diese Sicherheitslücke wurde bereits vorab im Rahmen der Vulnerability-Disclosure-Schreiben mitgeteilt:

- LOWTEQ_PDMS_ VU_2022/03: SQL-Injection – Patienten-Suchfunktion

Beschreibung von LOWTEQ_PDMS_ VU_2022/03

Generell ist die Kommunikation des PDMS mit der Datenbank gegen SQL-Injections abgesichert. Der Patienten-Suchdialog und der Protokoll-Ladedialog sind hier die Ausnahme, da an dieser Stelle noch über das JDBC-Interface direkt SQL-Statements abgesetzt wurden.

Diese Sicherheitslücke erfordert, dass der Angreifer physikalischen Zugriff auf die Clients hat, auf denen das PDMS installiert ist. Zusätzlich muss der Angreifer sich sowohl unter Windows als auch im PDMS authentifizieren und den Suchdialog öffnen. Der Angreifer benötigt weiter Kenntnisse in SQL und wir SQL-Statements für Injections zu formulieren sind.

Widdersdorfer Str. 236 - 240
50825 Köln
T +49 221 502946-0
F +49 221 502946-29
info@lowteq.de
www.lowteq.de
Ust-Id Nr.: DE223532894
St.-Nr. 217/5759/1068
Handelsregister Köln
HRB 38314
IBAN: DE75 4401 0046 0811 8164 60
BIC: PBNKDEFFXXX | Postbank

Auswirkungen

Eine SQL-Injection ermöglicht es einem Angreifer, Datenbankinhalte zu lesen, zu schreiben oder zu manipulieren. Der Angriff wird über die Eingabefelder des Suchdialogs ausgeführt. Der Angreifer manipuliert einen SQL-Befehl mithilfe von Sonderzeichen, wodurch eine Umgehung der Authentifizierung oder die Manipulation/Ausgabe von Datenbankeinträgen ermöglicht wird. Es ist einem Angreifer möglich, Daten aus der Datenbank auszulesen, zu verändern und zu löschen.

Risiken

Das Risiko für Patienten ist aufgrund des sehr spezifischen Angriffsszenarios, welches sowohl Zugriff auf die interne Netzwerkinfrastruktur erfordert, als auch sehr spezifische Kenntnisse als **Mittel** eingestuft.

Die CVSS 3.1 Scores für diese Sicherheitslücke (berechnet mit NVD - CVSS v3 Calculator) sind 6.7 (Base) und 6.2 (Temporal), Overall 6.4: Medium. (siehe CVSS v3.1 Specification Document)

AV:P/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:L/E:F/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:P/MAC:H/MPR:H/MUI:R/MS:C/MC:H/MI:H/MA:N

Es besteht kein Risiko für bereits behandelte Patienten, Anwender oder Dritte.

Welche Maßnahmen sind durch den Adressaten zu ergreifen

Es muss ein Update von LOWTeq*pdms* auf die Versionen 7.24.03 oder höher durchgeführt werden.

In der Zwischenzeit sind keine zusätzlichen Maßnahmen zu ergreifen. Der Betrieb von LOWTeq*pdms* ist sicher. Das Update wird in Absprache mit Ihnen im Rahmen der üblichen Updatezyklen durchgeführt, spätestens aber bis Ende 2022.

Weitergabe der hier beschriebenen Informationen

Bitte stellen Sie in Ihrer Organisation sicher, dass alle Anwender von LOWTeq*pdms* 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.

Widdersdorfer Str. 236 - 240
50825 Köln

T +49 221 502946-0
F +49 221 502946-29

info@lowteq.de
www.lowteq.de

Ust-Id Nr.: DE223532894
St.-Nr. 217/5759/1068

Handelsregister Köln
HRB 38314

IBAN: DE75 4401 0046 0811 8164 60
BIC: PBNKDEFFXXX | Postbank

Kontaktperson

Ansprechpartner ist der Leiter des Supports: Herr Andreas Heidenreich
Herr Heidenreich ist über die Support-Mailadresse zu erreichen, die angegebene Telefonnummer ist 24 Stunden am Tag besetzt-

Dr. Aloys Oberthür
Geschäftsführer LOWTeq GmbH - QMB

Widdersdorfer Str. 236 - 240
50825 Köln

T +49 221 502946-0
F +49 221 502946-29

info@lowteq.de
www.lowteq.de

Ust-Id Nr.: DE223532894
St.-Nr. 217/5759/1068

Handelsregister Köln
HRB 38314

IBAN: DE75 4401 0046 0811 8164 60
BIC: PBNKDEFFXXX | Postbank