**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*.

## 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_2022/02: Security Misconfiguration- SMB-Shares

### Beschreibung von LOWTEQ_PDMS_ VU_2022/02

In den SMB-Shares werden vor allem die Konfigurationsdaten des PDMS (Regeln, Scores, Abrechnungskataloge) und die zu verteilenden PDMS-Archive abgelegt. Ggf. werden hier auch die .pdf-Dokumente für den Versand durch die Schnittstellen abgelegt. Diese SMB-Shares sind zum Teil unzureichend gegen unberechtigten Zugriff geschützt.

Diese Sicherheitslücke erfordert, dass der Angreifer in das abgeschlossene Kliniksnetz eingedrungen ist und den Zugriff auf den Server hat, auf dem die SMB-Shares eingerichtet 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

Durch Schreibzugriff auf Netzlaufwerke kann z.B. Malware auf die Systeme des Kunden eingebracht werden. Jeder Mitarbeiter der auf diese Daten (z.B. Anwendungsdaten im Ordner Client) zugreift, kann dann sein System für den Angreifer öffnen.

## Risiken

Das Risiko für Patienten ist aufgrund des sehr spezifischen Angriffszenarios, welches sowohl Zugriff auf die interne Netzwerkinfrastruktur erfordert, als auch sehr spezifische Kenntnisse bei geringer Schadensschwere als **Niedrig** eingestuft.

Die CVSS 3.1 Scores für diese Sicherheitslücke (berechnet mit NVD - CVSS v3 Calculator) sind 5.9 (Base) und 5.5 (Temporal), Overall (3.6). Low. (siehe CVSS v3.1 Specification Document)

AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L/E:F/RL:O/RC:C/CR:M/IR:L/AR:M/MAV:N/MAC:L/MPR:H/MUI:R/MS:C/MC:N/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 eine konfigurative Änderung zur Absicherung der SMB-Shares durchgeführt werden. Die genaue Anleitung zur Durchführung liegt dieser Sicherheitsinformation bei.

In der Zwischenzeit sind keine zusätzlichen Maßnahmen zu ergreifen. Der Betrieb von LOWTeq*pdms* ist sicher. Die konfigurative Änderung kann unabhängig von Updates durch Sie durchgeführt werden.

## 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