LOWTeq GmbH | Widdersdorfer Strasse 236 - 240 | 50825 Cologne

Cologne the 16.09.2022

Urgent safety information

Security patches for
LOWTeqpdms

Sender

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

Addressee

IT departments of the customers of LOWTeq

Identification of the medical devices concerned

Affected are all versions of LOWTeqpdms up to version 7.24.02. Higher versions are not affected.

Description of the problem including the identified cause

In the course of a security test (also penetration test) a vulnerability in LOWTeqpdms was identified. This vulnerability was already disclosed in advance in the vulnerability disclosure letters:

- LOWTEQ_PDMS_ VU_2022/03 : SQL injection - patient search function

Description of LOWTEQ_PDMS_ VU_2022/03

In general, the communication of the PDMS with the database is protected against SQL injections. The patient search dialog and the protocol load dialog are the exception here, since SQL statements are still sent directly via the JDBC interface at this point.

This vulnerability requires that the attacker has physical access to the clients on which the PDMS is installed. In addition, the attacker must authenticate on both Windows and PDMS and open the search dialog. The attacker also needs knowledge of SQL and how to formulate SQL statements for injections.

Impact

An SQL injection allows an attacker to read, write or manipulate database contents. The attack is executed via the input fields of the search dialog. The attacker manipulates an SQL command using special characters, allowing authentication bypass or database manipulation. It is possible for an attacker to read modify and delete data from the database.

Risks

The risk for patients is graded due to the very specific attack scenario, which requires both access to the internal network infrastructure and very specific knowledge as a **medium.**

The CVSS 3.1 scores for this vulnerability (calculated with NVD - CVSS v3 Calculator) are 6.7 (Base) and 6.2 (Temporal), Overall 6.4: Medium. (see 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

There is no risk for already treated patients, users or third parties.

What measures are to be taken by the addressee

You have to update LOWTeqpdms to version 7.24.03 or higher.

In the meantime, no additional measures need to be taken. The operation of LOWTeqpdms is safe. The update will be carried out in consultation with you as part of the usual update cycles, but at the latest by the end of 2022.

Disclosure of the information described herein

Please ensure that all users of LOWTeqpdms and other persons to be informed are made aware of this **Urgent Safety Information.** If you have given the products to third parties, please forward a copy of this information or inform the contact person indicated below.

Please keep this information at least until the action has been completed.
The Bundesinstitut für Arzneimittel und Medizinprodukte has received a copy of this "Urgent Safety Information".

Contact

Contact person is the head of support: Mr. Andreas Heidenreich
Mr. Heidenreich can be reached via the support e-mail address, the telephone number given is manned 24 hours a day-.

[redacted]