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

All versions of LOWTeqpdms are 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_2022/01: Remote Code Execution - Java RMI

Description of LOWTEQ_PDMS_VU_2022/01

The business logic for DRG billing runs in the GlassFish application server. In addition, the ActiveMQ message queue is integrated into the GlassFish application server, via which the synchronization of the PDMS clients with each other (in multiple access) is implemented.

Due to an insecure configuration of the Java JMX interface, it is possible to install custom Java classes on on the server and execute it. Due to the disabled "com.sun.management.jmxremote.
authenticate" function, no authentication is required and an attacker can access the Java JMX interface.

This vulnerability requires that the attacker has penetrated the internal network and has access to the server where GlassFish is installed. Additionally, the code must be uploaded to be executed and the attacker must know how the specific function to load the classes is to be invoked.

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

Impact

Remote code execution allows an attacker to execute code from the server. This makes it possible to take over the system completely.

Risks

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

The CVSS 3.1 scores for this vulnerability (calculated with NVD - CVSS v3 Calculator) are 6.4 (Base) and 5.9 (Temporal), Overall 6.3: Medium. (see CVSS v3.1 Specification Document)
AV:L/AC:H/PR:H/UI:R/S:C/C:L/I:H/A:L/E:F/RL:O/RC:C/CR:M/IR:M/AR:M/MAV:N/MAC:H/MPR:H/MUI:R/MS:C/MC:L/MI:H/MA:L

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

What measures are to be taken by the addressee

A configurational change must be made to secure the SMB shares. The detailed instructions for performing this are enclosed with this security information.
In the meantime, no additional measures need to be taken. The operation of LOWTeqpdms is safe.
The configurational change can be done by you independently of updates.

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 listed 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".

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

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-.

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