1.10.2021

Safety Information custo diagnostic

custo diagnostic uses the open source application server "Apache Tomcat®", on which the actual custo diagnostic server is executed. When installing the custo diagnostic server, a version of Apache Tomcat® delivered by custo med is automatically installed and configured accordingly.

A security vulnerability has been reported for Apache Tomcat® versions from 8.5.0 up to and including 8.5.63 that we ship:

- CVE-2021-41079: Apache Tomcat 8.5.0 to 8.5.63, 9.0.0-M1 to 9.0.43 and 10.0.0-M1 to 10.0.2 did not properly validate incoming TLS packets. When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service.

  CVSS score: not yet known
  Further information: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41079

Affected custo med products

- custo diagnostic server up to version 5.4.4 or 5.5.1
- all custo diagnostic server versions 5.0.x to 5.3.x

In addition, custo diagnostic servers that were updated from a previous version **without reinstalling the server** are affected.

Information about the vulnerability

The listed vulnerability affects the encrypted communication between custo diagnostic server and custo diagnostic clients or between two custo diagnostic servers (e.g. for data exchange between senders and evaluation centers, mobile solutions, branch offices). Manipulated https packets can bring the server to a standstill or crash (denial of service attack). According to the current status, unauthorized intrusion into the server through this vulnerability is not possible.

Systems that can be accessed from outside (i.e. especially evaluation centers) are particularly at risk. In principle, however, all installations that use SSL for encryption during data transmission are affected.

Remedy

To fix the vulnerability, a complete reinstallation of the installed custo diagnostic server with a newer version (at least 5.4.5 or 5.5.2) is necessary. Please refer to our installation instructions. Customer or patient data will not be lost during this process. It may be necessary to restart the server computer system.

Note: Updating the custo diagnostic server (i.e. without uninstalling the previous version) is not sufficient!

Please take care of an appropriate data backup before starting to work on the system!

Please note the changed data format for Holter ECGs as from custo diagnostic version 5.5.1 and the compatibility notes for the respective version.

If you have any questions, please do not hesitate to contact us by e-mail (service@customed.de) or by phone at +49 - 89 - 71098-222.