1.10.2021

Sicherheitsinformation custo diagnostic

custo diagnostic verwendet den quelloffenen Applikationsserver „Apache Tomcat®“, auf dem der eigentliche custo diagnostic server ausgeführt wird. Bei der Installation des custo diagnostic server‘s wird automatisch eine von custo med ausgelieferte Version des Apache Tomcat® installiert und entsprechend konfiguriert.

Für von uns ausgelieferte Apache Tomcat®-Versionen von 8.5.0 bis einschließlich 8.5.63 wurde eine Sicherheitsschwachstelle gemeldet:

- 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: noch nicht bekannt
  Weitere Informationen: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41079

Betroffene custo med-Produkte

- custo diagnostic server bis Version 5.4.4 oder 5.5.1
- alle custo diagnostic server-Versionen 5.0.x bis 5.3.x

Außerdem sind custo diagnostic server betroffen, die von einer früheren Version **ohne Neuinstallation des Servers** aktualisiert wurden.

Hinweise zur Schwachstelle

Die aufgeführte Schwachstelle betrifft die verschlüsselte Kommunikation zwischen custo diagnostic server und custo diagnostic clients bzw. zwischen zwei custo diagnostic servern (z.B. bei Datenaustausch zwischen Zusendern und Auswertezentralen, mobilen Lösungen, Filialpraxen). Manipulierte https-Pakete können den Server zum Stillstand bzw. zum Absturz bringen (Denial of Service-Attacke). Ein unberechtigtes Eindringen in den Server durch diese Schwachstelle ist nach derzeitigem Stand nicht möglich.

Besonders gefährdet sind Systeme, welche von außen erreichbar sind (d.h. insbesondere Auswertezentralen). Grundsätzlich sind allerdings alle Installationen betroffen, bei denen SSL zur Verschlüsselung bei der Datenübertragung zum Einsatz kommt.

Abhilfe

Zur Behebung der Schwachstelle ist eine komplette Neuinstallation des installierten custo diagnostic servers mit einer neueren Version (mindestens 5.4.5 bzw. 5.5.2) notwendig. Bitte beachten Sie dazu unsere Hinweise zur Installation. Kunden- oder Patienten-Daten gehen bei diesem Vorgang nicht verloren! Ggf. ist ein Neustart des Server-Computersystems nötig.
Hinweis: Eine Aktualisierung des custo diagnostic server‘s (d.h. ohne Deinstallation der bisherigen Version) ist nicht ausreichend!

Bitte kümmern Sie sich vor Beginn der Arbeiten am System um eine entsprechende Datensicherung!

Bitte beachten Sie das geänderte Datenformat für Langzeit-EKGs ab der Version 5.5.1 der custo diagnostic sowie die Kompatibilitätshinweise für die jeweilige Version.

Für Fragen hierzu stehen wir Ihnen gerne per E-Mail (service@customed.de) oder telefonisch unter 089 / 71098-222 zur Verfügung.