Ottobrunn, 13.12.2021

Sicherheitsinformation custo diagnostic

Die Softwarekomponente „log4j“ ist eine beliebte Protokollierungsbibliothek für Java-Anwendungen. Sie dient der performanten Aggregation von Protokolldaten einer Anwendung. Der custo diagnostic server verwendet diese Bibliothek ebenfalls um Logeinträge zu erstellen.

Für die von uns ausgelieferte Version log4j in Version 2.13.3 wurde eine Sicherheitslücke gemeldet:

- CVE-2021-44228
  Apache Log4j2 <=2.14.1 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enable

  CVSS-Score: 10.0
  BSI IT-Bedrohungslage: 4 / ROT (Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden)

  Weitere Informationen:
  https://nvd.nist.gov/vuln/detail/CVE-2021-44228
  https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf

Betroffene custo med-Produkte:

- Alle custo diagnostic server Versionen
  - 5.4.0 bis 5.4.7 (Behoben in 5.4.8)
  - 5.5.0 bis 5.5.6 (Behoben in 5.5.7)
  - 5.6.0 bis 5.6.2 (Behoben in 5.6.3)
- Ältere Versionen haben diese Sicherheitslücke nicht, da noch eine ältere Log4J Version ausgeliefert wurde. Wir empfehlen trotzdem ein Update auf eine aktuelle Version, in der die Sicherheitslücke geschlossen wurde.

Hinweise zur Sicherheitslücke:

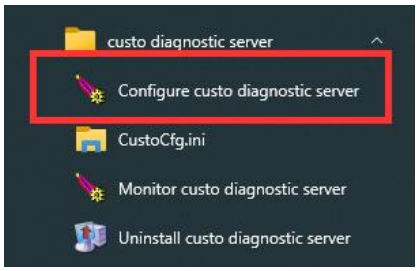
Die aufgeführte Sicherheitslücke betrifft die Ausgabe von Benutzereingaben in den Logdateien. Durch speziell formatierte Aufrufe, oder auch speziell formatierte Nachrichten über HL7/DICOM ist es Angreifern auch ohne Login möglich, Schadcode auf das Zielsystem (custo diagnostic server) zu laden, dort auszuführen und den Server zu kompromittieren.
Besonders gefährdet sind Systeme, welche von außen erreichbar sind (d.h. insbesondere Auswertezentralen). Grundsätzlich sind allerdings alle Installationen betroffen, vor allem bei Netzwerkbetrieb oder Nutzung einer Kommunikationsschnittstelle (HL7 / DICOM).
Bei Systemen, welche nur rein intern oder ohne weitere Kommunikationsschnittstellen betrieben werden, besteht eine deutlich geringere Gefährdung, wir raten allerdings trotzdem zur Umsetzung der beschriebenen Maßnahmen.

Abhilfe:

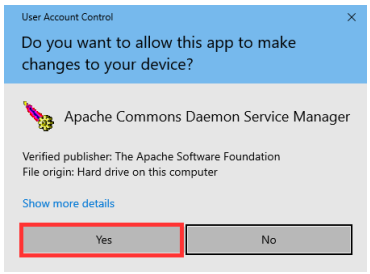
Zur Behebung der Schwachstelle ist ein Update des custo diagnostic-Servers mindestens auf die Versionen 5.4.8, 5.5.7 oder 5.6.3 (in Abhängigkeit der vorhandenen Lizenz) notwendig. Das Update kann ohne vorherige Deinstallation der vorherigen Version des Servers durchgeführt werden. Wir empfehlen aber eine komplette Neuinstallation, falls der Apache Tomcat nicht in der aktuellen Version 8.5.73 installiert ist.
Bitte beachten Sie dazu unsere Hinweise zur Installation, Kunden- oder Patienten-Daten gehen bei ordnungsgemäßen Updatevorgang nicht verloren! Ggf. ist ein Neustart des Server-Computersystems nötig.

Als Sofortmaßnahme bis zum erfolgten Update des custo diagnostic-Servers sollte folgende Maßnahme ergriffen werden:
Setzen der Option "**log4j2.formatMsgNoLookups**" auf "**true**" bei den Java-Optionen des custo diagnostic-Servers.

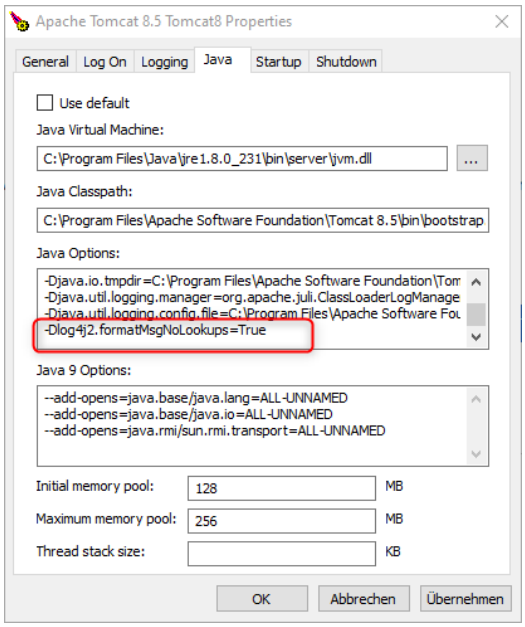
Die Konfiguration des Apache Tomcats können Sie über das Programm **„Configure custo diagnostic server“** auf dem Serversystem bzw. dem Rechner, auf dem der custo diagnostic-Server ausgeführt wird aufrufen. Sie finden dieses unter „custo diagnostic server“ im Startmenü:



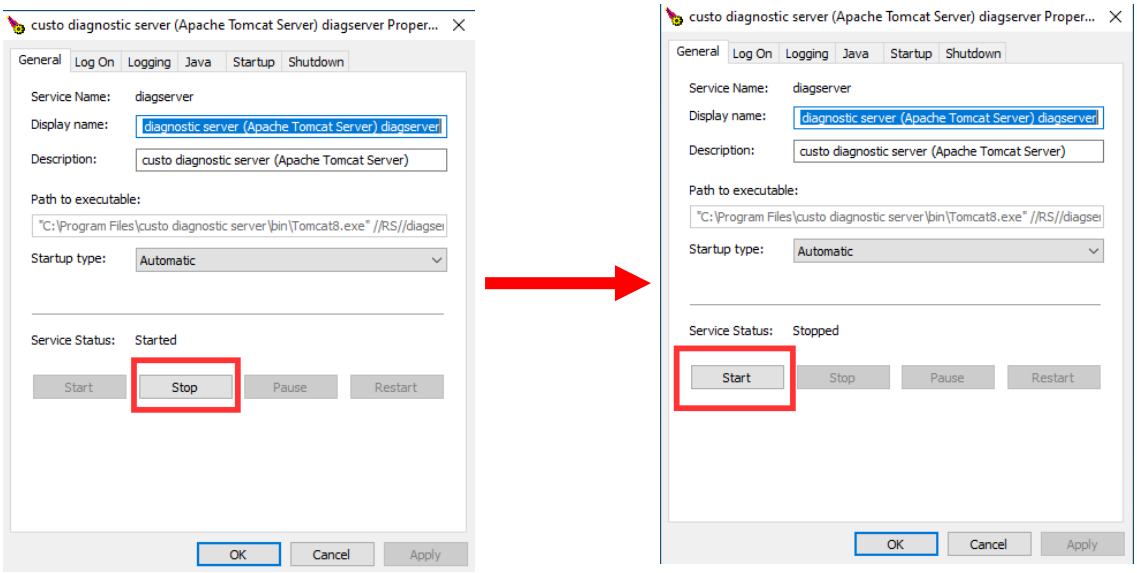
Sollte eine Sicherheitsabfrage von Microsoft Windows erscheinen, diese bitte mit „Ja“ bestätigen:



Im Reiter „Java“ kann der entsprechende Parameter „`-Dlog4j2.formatMsgNoLookups=True`“ ergänzt werden:



Bitte bestätigen Sie diese Anpassung mit dem Button „Übernehmen“ und starten im Anschluss den custo diagnostic-Server über die Schaltflächen „Stoppen“ und „Starten“ (bzw. „Neustart) im Reiter „Allgemein“ neu:



Je nach Systemkonfiguration kann es etwas dauern, bis der custo diagnostic-Server in den Status „gestoppt“ wechselt, als Alternative dazu ist auch der komplette Neustart des betreffenden Rechners möglich.

Als weitere Möglichkeit kann noch die Systemvariable „LOG4J_FORMAT_MSG_NO_LOOKUPS“ auf „true“ gesetzt werden (`LOG4J_FORMAT_MSG_NO_LOOKUPS = true`), auch hier ist ein Neustart des custo diagnostic-Servers oder des kompletten Rechners notwendig.

Im Anschluss daran ist wieder ein normales Arbeiten mit dem custo diagnostic System möglich, bei Fragen steht Ihnen Ihr autorisierter custo med Fachhandelspartner oder unsere Hotline (erreichbar per Mail an service@customed.de oder telefonisch unter 089 / 71098-222) zur Verfügung.

12/2021

custo med GmbH
85521 Ottobrunn