

INFO PAPER

SCHWACHSTELLE LOG4SHELL

Analyseergebnis, Empfehlungen und Anleitung

- Schwachstelle in der Java log4j-Bibliothek
- Betroffene PCS Produkte
- Analyseergebnis und Empfehlungen
- Absicherung des DEXICON AMS-OSS-Driver
- Absicherung des DEXICON AMS-Kernel
- Absicherung des INTUS COM HTTPS-Server



Durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist der Hinweis auf eine kritische Schwachstelle in der Java log4j-Bibliothek veröffentlicht worden.

Diese Bibliothek wird auch in DEXICON 5.4, sowie dem HTTPS-Server von INTUS COM 3.4 und INTUS COM 3.5 eingesetzt. PCS empfiehlt den Nutzern von DEXICON 5.4 und INTUS COM 3.4/3, die Schwachstelle adhoc zu schließen.

Dazu ist bei DEXICON 5.4 der AMS-OSS-Driver und der AMS-Kernel, sowie bei INTUS COM 3.4/3.5 der INTUS COM HTTPS Server abzusichern, indem die system property log4j2.formatMsgNoLookups auf true eingestellt wird.

Auf Seite 2 finden Sie die Schritt-für-Schritt Anleitung dazu.

Absicherung des DEXICON AMS-OSS-Driver

1. AMS-OSS-Driver beenden.
2. Das Batchfile „<Installationspfad>\Dexicon-ams\bin\ams_oss_driver\yajsw\bat\uninstallService.bat“ ausführen.

(Standardinstallationspfad=“C:\Program Files (x86)\PCS-Systemtechnik“).
3. In der Datei „<Installationspfad>\Dexicon-Ams\bin\ams_oss_driver\yajsw\conf\wrapper.conf“ im Abschnitt „# Wrapper Windows Service and Posix Daemon Properties“ den folgenden Eintrag hinzufügen:

wrapper.ntservice.additional.<n> = -Dlog4j2.formatMsgNoLookups=true

Dabei ist <n> = die Anzahl der, in der Datei vorhandenen und nicht auskommentieren Einträge „wrapper.ntservice.additional.“ + 1

Ist kein Eintrag „wrapper.ntservice.additional.“ vorhanden, so ist <n> = 1

(wrapper.ntservice.additional.1 = -Dlog4j2.formatMsgNoLookups=true).
4. Und im Abschnitt „# Java/Groovy Application Properties“ den folgenden Eintrag hinzufügen:

wrapper.java.additional.<n>=-Dlog4j2.formatMsgNoLookups=true

Dabei ist <n> = die Anzahl der, in der Datei vorhandenen und nicht auskommentieren Einträge „wrapper.java.additional.“ + 1

Ist kein Eintrag „wrapper.java.additional.“ vorhanden, so ist <n> = 1

(wrapper.java.additional.1=-Dlog4j2.formatMsgNoLookups=true).
5. Das Batchfile „<Installationspfad>\Dexicon-Ams\bin\ams_oss_driver\yajsw\bat\installService.bat“ ausführen.
6. AMS-OSS-Driver starten.

Absicherung des DEXICON AMS-Kernel

1. AMS-Kernel beenden.
2. Das Batchfile „<Installationspfad>\Dexicon-Ams\bin\ams_kernel\yajsw\bat\uninstallService.bat“ ausführen.

(Standardinstallationspfad=“C:\Program Files (x86)\PCS-Systemtechnik“).
3. In der Datei „<Installationspfad>\Dexicon-Ams\bin\ams_kernel\yajsw\conf\wrapper.conf“ im Abschnitt „# Wrapper Windows Service and Posix Daemon Properties“ den folgenden Eintrag hinzufügen:

wrapper.ntservice.additional.<n> = -Dlog4j2.formatMsgNoLookups=true

Dabei ist <n> = die Anzahl der, in der Datei vorhandenen und nicht auskommentieren Einträge „wrapper.ntservice.additional.“ + 1

Ist kein Eintrag „wrapper.ntservice.additional.“ vorhanden, so ist <n> = 1

(wrapper.ntservice.additional.1 = -Dlog4j2.formatMsgNoLookups=true).

4. Und im Abschnitt „# Java/Groovy Application Properties“ den folgenden Eintrag hinzufügen:

wrapper.java.additional.<n>=-Dlog4j2.formatMsgNoLookups=true

Dabei ist <n> = die Anzahl der, in der Datei vorhandenen und nicht auskommentieren Einträge „wrapper.java.additional.“ + 1

Ist kein Eintrag „wrapper.java.additional.“ vorhanden, so ist <n> = 1

(wrapper.java.additional.1=-Dlog4j2.formatMsgNoLookups=true).

5. Das Batchfile „<Installationspfad>\Dexicon-Ams\bin\ams_kernel\yajsw\bat\installService.bat“ ausführen.
6. AMS-Kernel starten.

Absicherung des INTUS COM HTTPS-Server

1. INTUS COM HTTPS-Server beenden.
2. Das Batchfile „<Installationspfad>\Intuscom\bin\https_server\yajsw\bat\uninstallService.bat“ ausführen.

(Standardinstallationspfad=“C:\Program Files (x86)\PCS-Systemtechnik“).
3. In der Datei „<Installationspfad>\Intuscom\bin\https_server\yajsw\conf\wrapper.conf“ im Abschnitt „# Wrapper Windows Service and Posix Daemon Properties“ den folgenden Eintrag hinzufügen:

wrapper.ntservice.additional.<n> = -Dlog4j2.formatMsgNoLookups=true

Dabei ist <n> = die Anzahl der, in der Datei vorhandenen und nicht auskommentieren Einträge „wrapper.ntservice.additional.“ + 1

Ist kein Eintrag „wrapper.ntservice.additional.“ vorhanden, so ist <n> = 1

(wrapper.ntservice.additional.1 = -Dlog4j2.formatMsgNoLookups=true).
4. Und im Abschnitt „# Java/Groovy Application Properties“ den folgenden Eintrag hinzufügen:

wrapper.java.additional.<n>=-Dlog4j2.formatMsgNoLookups=true

Dabei ist <n> = die Anzahl der, in der Datei vorhandenen und nicht auskommentieren Einträge „wrapper.java.additional.“ + 1

Ist kein Eintrag „wrapper.java.additional.“ vorhanden, so ist <n> = 1

(wrapper.java.additional.1=-Dlog4j2.formatMsgNoLookups=true).
5. Das Batchfile „<Installationspfad>\Intuscom\bin\https_server\yajsw\bat\installService.bat“ ausführen.
6. INTUS COM HTTPS-Server starten.

© 2021-12 PCS Systemtechnik GmbH

PCS, INTUS und DEXICON sind eingetragene Marken der PCS Systemtechnik GmbH.
Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen und Organisationen.

PCS Systemtechnik GmbH · Pfälzer-Wald-Str. 36 · 81539 München · Tel. +49 89 68004-0
Ruhrallee 311 · 45136 Essen · Tel. +49 201 89416-0
intus@pcs.com · www.pcs.com

