Beratung und Support
Technische Plattform
Support-Netz-Portal

paedML® – stabil und zuverlässig vernetzen

Anleitung

log4j-Sicherheitslücken in der paedML Novell 4.3 und 4.4 schließen

Stand 17.12.2021

paedML® Novell

Version: paedML Novell 4.3 und 4.4

paedML N

lmz Landesmedienzentrum Baden-Württemberg

Impressum

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)
Support-Netz
Rotenbergstraße 111

70190 Stuttgart

Autoren

der Zentralen Expertengruppe Netze (ZEN),

Holger Dzeik
Stefan Falk
Ulrich Frei
Carl Heinz Gutjahr
Stephan Kluge
Uwe Labs
Steffen Rahn
Till Eberlein
Alfred Wackler

Endredaktion

Alfred Wackler

Bildnachweis

Symbole von “The Noun Project” (www.thenounproject.com)

Weitere Informationen

www.lmz-bw.de

Änderungen und Irrtümer vorbehalten.

Veröffentlicht: 2021

Inhaltsverzeichnis

Vorwort

Als unpassendes Weihnachtsgeschenk hat uns die Welt die log4j-Sicherheitslücke CVE-2021-44228 beschert. Glücklicherweise ist die paedML Novell nur recht eingeschränkt betroffen.

Nicht betroffen lt. Micro Focus sind:

- OES 2018 (bei uns der GServer03 incl. iPrint)
- GroupWise Mobility Service
- KServer (bei uns Vibe)
- Filr

Betroffen sind aber:

- GroupWise (nur in den mit der paedML Novell 4.3 und 4.4 ausgelieferten Versionen! GroupWise 2014, das mit der Version 4.2 ausgeliefert wurde, ist nach aktuellem Kenntnisstand nicht betroffen)
- ZServer (ZCM 2020 U1. U2 wurde noch nicht freigegeben. ZCM 2017 ist nicht betroffen)

Bei GroupWise ist nur betroffen:

- GW Admin Console
- GW Messenger (sofern installiert)
- GW Calendar Server (sofern für Mac-Kalender-Zwecke überhaupt benutzt)

Sicher wird es von Micro Focus Updates für die betroffenen Produkte geben. Diese müssen aber erst getestet werden, was möglicherweise etwas dauert. Wer auf „Nummer sicher“ gehen will, der kann aber die Sicherheitslücke mit einigen Befehlen eindämmen.

Bei Micro Focus gibt es die Seite
https://portal.microfocus.com/s/customportalsearch?language=en_US&searchtext=CVE-2021-44228,
die alle(!) Produkte mit ihrer log4j-Gefährdungslage enthält.

Bei den folgenden Schritten zur Behebung der Sicherheitslücke gehen wir von einer paedML Novell der Versionen 4.4 oder die folgende. Unsere Schritte zur Schließung der Sicherheitslücke sind trotz der Eile sorgfältig zusammengestellt, eine Garantie, dass damit die Gefährdung 100%ig beseitigt ist, maßen wir uns aber nicht an. Bei älteren Versionen der paedML Novell müssen ggf. die Dateinamen der log4j-Dateien angepasst werden.

1 Sicherheitslücken schließen

1.1 GroupWise

GW WebAccess ist lt. Micro Focus nicht betroffen.

Normalerweise dürfte die GW Admin Console von außen gar nicht erreichbar sein. Daher sollte die Gefährdungslage eher gering sein, soweit man von Angriffen von innen einmal absieht.

Der GW Calendar Server ist bei uns zwar installiert, aber nicht konfiguriert. Da dieser Serverdienst nur im Zusammenhang mit dem Kalenderfunktionen für (Apple-) Mac von Interesse ist, werden vermutlich nur wenige Schulen diesen Dienst tatsächlich benutzen.

Auch der GW Messenger ist vermutlich eher selten in Benutzung.

Trotzdem geben wir nun die nötigen Schritte an. Micro Focus gibt hierzu die GW-Versionen von 18.0 bis 18.3.1 an. Loggen Sie sich als *root* auf dem GServer03 ein. Besonders angenehm ist die Verwendung von Putty, da dann die unten genannten Befehle per Drag&Drop in das Putty-Fenster (mit der rechten Maustaste) übertragen werden können. Sollten dabei die Bindestriche beim Ausführen der Befehle ein Problem darstellen, können diese einfach in der Kommandozeile korrigiert werden. So, nun aber „zur Sache“:

Hinweis: Im folgenden Befehlsblock löscht der zweite *zip*-Befehl eine bestimmte Zeile aus der *log4j-core-2.12.0.jar*-Datei. Die Versionsnummer dieser Datei (*2.12.0*) ist abhängig von der eingesetzten Version von GroupWise. Um diese Nummer zu ermitteln, wird der *ll log4j**-Befehl (siehe unten) verwendet, damit der korrekte *zip*-Befehl abgesetzt werden kann.

GW Admin Console

```
cd /opt/novell/groupwise/admin/lib
zip -q -d log4j-core.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
cd /opt/novell/groupwise/admin/webapps
chmod -R 0775 ./gwadmin-console
cd gwadmin-console/WEB-INF/lib
ll log4j*
zip -q -d log4j-core-2.12.0.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
cd /opt/novell/groupwise/admin/webapps
chmod -R 0555 ./gwadmin-console
```

GW Calendar Server

```
cd /opt/novell/groupwise/calsvr/runner/lib
zip -q -d log4j-core-2.11.0.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
```

Bitte auch hier die log4j-core-Version überprüfen!

GW Messenger

```
cd /opt/novell/messenger/bin
zip -d mars.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
systemctl restart gwm-mars@gwmsgr.service
```

1.2 ZServer / ZCM

Die Versionen ZCM 2017, 2020.0 sind nicht betroffen. Die Version 2020 U1 und 2020 U2 sind betroffen, wobei wir in der paedML Novell z.Z. auf dem Stand 2020 U1 (unter SLES 11.4) sind.

Haben Sie also ZCM 2020 U1 auf SLES 11.4 vorliegen, gehen Sie zum Schließen der Sicherheitslücke folgendermaßen vor. Loggen Sie sich als *root* auf dem ZServer ein, am besten wieder per Putty (siehe oben).

Wechseln Sie ins Verzeichnis */etc/profile.d* und erzeugen dort die Datei *log4jEnvironmentVariable.sh*:

```
cd /etc/profile.d/
touch log4jEnvironmentVariable.sh
```

Editieren Sie diese Datei und geben dort die Zeile

```
export LOG4J_FORMAT_MSG_NO_LOOKUPS=true
```

ein. Speichern Sie ab.

Loggen Sie sich aus und anschließend wieder als *root* ein (wir laut Originaldokumentation von Microfocus so vorgegeben!).

Geben Sie folgenden Befehl ein

```
novell-zenworks-configure -c Start
```

und wählen Sie Restart (also 15 eingeben) → Enter → Enter.

2 Schluss

Damit wären die benötigten Maßnahmen für's Erste durchgeführt. Sobald neue Updates/Patches von Micro Focus verfügbar sind, werden wir darauf reagieren.

Viel Erfolg auch weiterhin mit der nun "gehärteten" paedML Novell,

Ihre ZEN Novell.

Landesmedienzentrum Baden-Württemberg (LMZ)
Support Netz
Rotenbergstraße 111

70190 Stuttgart

paedML N

LMZ Landesmedienzentrum Baden-Württemberg