Vulnerability in PREEvision

Log4Shell

Version	1.2 from 2021-12-21
Status	released
Autor	Vector Informatik
Copyright	2021 Vector Informatik GmbH

Document Versioning

Release

Role	Version	Date
Product Coordinator	1.2	2021-12-21
Architect	1.2	2021-12-21
Manager Operating	1.2	2021-12-21
Test Manager	1.2	2021-12-21

Revision list

Version	Date	Section	Changes, comments
0.1	2021-12-13	All	Created
1.0	2021-12-14	All	Review and release of the document.
1.1	2021-12-16	3.	Update of chapter 3: Solution for PREEvision 8.5, 9.0, 9.5, 10.0 and customized code Update of chapter 3.3: Changed recommendation for the PREEvision Monitoring Updated information based on CVE-2021-45046
1.2	2021-12-21	All	Updated information based on CVE-2021-45105 Planning information

Content

1 Summary

We inform you about the critical security vulnerability "Log4Shell" CVE-2021-44228, CVE-2021-45046 and CVE-2021-45105 for software components used in PREEvision.

A detailed description of the vulnerabilities can be found here:

CVE-2021-44228

CVE-2021-45046

CVE-2021-45105

An attacker could use the security gap by sending manipulated requests to a vulnerable server or application.

Log4j2 <= 2.15 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 enabled.

2 Results of the Risk Analysis

Log4j is affected from version 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0.

The problem can be avoided in all 2.x version by removing the *JndiLookup* class from the library.

From version 2.15.0 the behavior was disabled by default but keeps a chance for denial-of-service attacks. The latest recommended safe version is 2.17.

Setting the Java/System parameter -D*log4j2.formatMsgNoLookups=true* can reduce the attack surface but does therefore not address all possible attack vectors.

Overall, we recommend following the instructions below.

CVE-2021-45105: We do not use Context Look-ups with the current versions of PREEvision. We will replace the version of the library in the next service packs of PREEvision 10.0 and PREEvision 9.5.

3 Resolution of the Issue for PREEvision

PREEvision 8.5.*, 9.0.*, 9.5.* and 10.0.* is using Log4J.

The following chapter are instruction on how to resolve the issue.

Please check also your customization in case you have integrated the component in your customized code (e.g. metric API using effected LOG4J library as external jar).

3.1 PREEvision 8.0, 8.5 and 9.0

Log4J is used on PREEvision Clients in the relevant version **2.5.0**. or version **2.4.0**.

Log4J is also used in version **1.*** without any *JMSAppender Configuration* in use. This library is not affected from this CVE.

Task 1: Use the patched Log4j2 libraries without the problematic class 'JndiLookup.class' from the Vector Download Center and follow the contained instructions: https://download.vector.com/servicepacks/preevision/log4j-patch-v1.2.0.zip

On PREEvision Collaboration Server no activity is needed because we are using version Log4J 1.2.15. This library is not affected from this CVE.

3.2 PREEvision 9.5

Log4J is used on PREEvision Clients in the relevant version **2.12.0.**

Task 1: Use the patched Log4j2 libraries without the problematic class 'JndiLookup.class' from the Vector Download Center and follow the contained instructions: https://download.vector.com/servicepacks/preevision/log4j-patch-v1.2.0.zip

Task 2: If Task 1 is not possible for you to rollout, we recommend at least setting the parameter

-Dlog4j2.formatMsgNoLookups=true

in the PREEvision.ini on the PREEvision Client to minimize the risk.

Log4J is also used in version **1.*** without any JMSAppender Configuration in use. This library is not affected from this CVE.

On PREEvision Collaboration Server (Messaging, Staging, Gateway, Application Server, API Server) no activity is needed because we are using version Log4J 1.2.15. This library is not affected from this CVE.

3.3 PREEvision 10.0

Log4J is used on PREEvision Clients in in the relevant version **2.12.0:**

Task 1: Use the patched Log4j2 libraries without the problematic class 'JndiLookup.class' from the Vector Download Center and follow the contained instructions: https://download.vector.com/servicepacks/preevision/log4j-patch-v1.2.0.zip

Task 2: If Task 1 is not possible for you to rollout, we recommend at least setting the parameter

-Dlog4j2.formatMsgNoLookups=true

in the PREEvision.ini on the PREEvision Client to minimize the risk.

Log4J is also used in version **1.*** without any JMSAppender Configuration in use. This library is not affected from this CVE.

Log4J **2.11.1** is used for the PREEvision Monitoring on server side.

The PREEvision Monitoring DataStorage is using the 3party component Elasticsearch.

A comment from the vendor: *"Elasticsearch is not susceptible to remote code execution with this vulnerability due to our use of the Java Security Manager, however we are making a fix available for an information leakage attack also associated with this vulnerability. Additional details below."*

https://github.com/YfryTchsGD/Log4jAttackSurface/blob/master/pages/ElasticSearch.md

https://opendistro.github.io/for-elasticsearch/blog/2021/12/update-to-1-13-3/

Task 3: Although the DataStorage component is not affected from this CVE, for minimizing the risk we recommend setting the parameter

-Dlog4j2.formatMsgNoLookups=true

in vCollabMonitoringDataStorage\config\jvm.options

For the other PREEvision server components:

No further change needed on PREEvision Collaboration Server (Messaging, Staging, Gateway, Application Server, API Server) because on server side we are using version Log4J 1.2.15. This library is not affected from this CVE.

4 Further Product Roadmap for PREEvision

Vector will provide updated versions of the product PREEvision:

4.1 PREEvision 9.5 SP12

A service pack is currently planned for 2022-01-20:

This service pack will include an update for the Log4J library version 2.* on all components (e.g. client, server, monitoring) but no change of the Log4J library version 1.*

The new version is at least 2.17.

4.2 PREEvision 10.0 SP6

A service pack is currently planned for 2022-01-26:

This service pack will include an update for the Log4J library version 2.* on all components (e.g. client, server, monitoring) but no change of the Log4J library version 1.*

The new version is at least 2.17.

4.3 PREEvision 10.5 or 11.0

A change for the Log4J library version 1.* needs a major release. A final planning is not done yet.

5 Contact

Please contact the support for any further question.

Vector Informatik GmbH
www.vector.com/contact
support@vector.com