

## Customer Notice

Published: December 15, 2021

### Apache Log4j Vulnerability Update

As you are maybe aware, a vulnerability has recently been identified related to the Apache Log4j logging framework. Log4j is an open source logging framework incorporated into many Java-based software applications.

This vulnerability is reported under the CVE ID: CVE- 2021-44228 and was released to the public on December 10, 2021.

Ciena has been analyzing this vulnerability to understand its impact on our products and services.

At this time, we are continuing to review our Blue Planet products. Based on the product and software version you are running, the tables below indicate whether we believe that the Log4j vulnerability is present and our mitigation recommendation where applicable.

We have updated our mitigation recommendation with regard to the java version used by the product as it is now deemed insufficient to mitigate the risk. As indicated below, we are recommending to mitigate the vulnerability by blocking LDAP requests going the internet.

Ciena is currently testing the products affected by the vulnerability to reproduce the exploit. This testing is still on-going, but so far we haven't been able to reproduce the exploit.

#### Blue Planet Inventory Product (BPI)

Product Release	Is the log4j vulnerability present ?	Recommendation
BPI__19.06	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
BPI__19.10	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
BPI__20.02	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
BPI__20.06	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
BPI__20.10	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
BPI__21.02	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
BPI__21.02	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
BPI__21.06	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet

## Blue Planet Orchestrate (BPO/SOO)

Product Release	Is the log4j vulnerability present ?	Recommendation
BPO__17.02	NO	No action required at this time
BPO__17.06	NO	No action required at this time
BPO__17.10	NO	No action required at this time
BPO__18.02	NO	No action required at this time
BPO__18.06	NO	No action required at this time
BPO__19.02	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
BPO__19.06	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
BPO__19.10	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
BPO__20.02	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
BPO__20.06	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
BPO__20.10	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
BPO__21.02	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
BPO__21.06	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet

## Blue Planet Unified Assurance & Analytics (UAA)

Product Release	Is the log4j vulnerability present ?	Recommendation
UAA__1.6-12	NO	No action required at this time
UAA__1.8-47	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
UAA__1.9-60	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
UAA__1.9-64	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
UAA__1.9-72	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
UAA__1.10-48	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
UAA__6.0-103	NO	No action required at this time
UAA__6.0-69	NO	No action required at this time
UAA__19.10	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
UAA__20.02	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
UAA__21.02	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
UAA__21.06	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet

## Blue Planet Route Optimization and Analytics (ROA)

Product Release	Is the log4j vulnerability present ?	Recommendation
ROA__REX-16.1	NO	No action required at this time
ROA__REX-17.1	NO	No action required at this time
ROA__REX-17.2	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
ROA__REX-17.3	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
ROA__REX-18.1	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
ROA__REX-18.2	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
ROA__REX-19.02	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
ROA__REX-19.06	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
ROA__REX-19.10	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
ROA__REX-20.02	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
ROA__REX-20.06	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
ROA__REX-20.10	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet
ROA__REX-21.02	YES	To mitigate the risk, Ciena recommends blocking LDAP requests going to internet

## Blue Planet Integration assets and customization

In some cases, it is possible that projects including customization and customer specific integration may include software assets that could be affected by this vulnerability. Ciena is still analyzing if the vulnerability is present in integration assets or project customizations and will provide updates when they become available.

## Mitigation and Remediation Plan

This update covers mitigation options for the Ciena Blue Planet products. The Ciena Blue Planet team is working on a further remediation plan and will be communicating the remediation plan as soon as it becomes available.

Updates about this vulnerability and mitigation will be published in the Ciena Blue Planet portal:

<https://my.ciena.com/CienaPortal/s/blue-planet>

If you have any questions, you contact our support by creating a ticket on the Ciena portal:

<https://my.ciena.com/CienaPortal/s/Ciena-Portal-Home>

The Blue Planet team