PIB - *Memorandum*

Supplier Information:	CIENA Corporation 7035 Ridge Road Hanover, MD 21076	**1. PIB No.**	PIB-M211214-101 Rev 2.0	**2. Date:** Dec 14, 2021

3. Title: Ciena Response to Apache Log4j Vulnerability (CVE-2021-44228)

4. **Product Line(s):** 5400, 6500, 8700, 38xx Family, 39xx Family, 51xx Family, 5400 Node Manager, 61xx Family, 6500 PTS, 6500 T-Series, 81xx Family, Ciena Node Manager (CNM), CPL, ELS, ESM, License Server, MCP, MyCryptoTool, NodeEssentials, OneControl, OnePlanner, Planet Operate, Planner Plus, RLS, Site Manager, Vyatta NOS, Waverserver 5, Waveserver, Waveserver AI and Z-Series	**5. Part Number(s) Affected:** N/A

Security Bulletin for Apache Log4j Vulnerability (CVE-2021-44228)

To: Ciena Customers and Partners

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.

The community has identified a remote code execution vulnerability, ultimately being reported under the CVE ID: CVE-2021-44228, released to the public on December 10, 2021.

Ciena is currently analyzing this vulnerability and we are assessing what impact, if any, there may be for our products and services.

Ciena Products Not Impacted by the Log4j vulnerability

The following products have been analyzed and have been found not to be impacted:

- 5400
- 6500
- 6500 -T series
- 6500 -PTS
- 8700
- 38xx Family
- 39xx Family
- 51xx Family
- 5400 Node Manager
- 81xx Family
- Ciena Node Manager (CNM)
- CPL
- ELS
- License Server
- MyCryptoTool
- NodeEssentials
- OneControl
- OnePlanner
- Planet Operate
- RLS

- Vyatta NOS
- Waverserver 5
- Waveserver
- Waveserver AI

Ciena Products Impacted by the Log4j vulnerability

- Manage Control Plan (MCP) Versions 4.x through 5.x
- Site Manager Versions 10.0 and above

Details of the Log4j vulnerability impact on MCP Versions 4.x through 5.x

Explanation of the Issue:

Ciena has analyzed the vulnerability and its effect on MCP. MCP is a server network management application accessed by clients via a web browser. MCP versions 4.x through 5.x include a vulnerable version of the Log4j utility.

Impact of the Issue:

At this point in our investigation, we believe the flaw is not exploitable.

We continue to monitor developments of the Log4j flaw and analyze any potential exposure MCP may have to this vulnerability.

Mitigations:

No mitigations required at this time.

Details of the Log4j vulnerability impact on Site Manager Versions 10.0 and higher

Explanation of the Issue:

Ciena has analyzed the vulnerability and its effect on Site Manager. Site Manager is a client-side application installed locally on individual workstations. The installation includes the vulnerable version of Log4j.

Impact of the Issue:

Ciena has determined that the impact of this vulnerability is **Low** and likelihood of attack is **Low**.

Unlike the remote code execution attack that is present on server-side services, and detailed in the CVE, in order for the vulnerability to be exploited in this scenario, the attacker would have to have authenticated access to the workstation and permission to the Site Manager directory and application. The exploit does not result in a privilege escalation, therefore the actions executed via this vulnerability would already be executable by the attacker given their access to the target workstation. If an attacker has this level of access to the workstation more direct attacks would be the preferred method.

Mitigations:

However, if users wish to eliminate the presence of the vulnerable 3rd Party library from the workstation, the following steps are recommended.

- Uninstall Site Manager from the system using the built-in operating system software management function

- Navigate to C:\Program Files and delete the folder Site Manager XX.YY, where XX.YY is the Site Manager version. For Example: C:\Program Files (x86)\Site Manager_12.72
- Note: For some older releases, the folder name may not include the version.
- Delete any copies of the installation file on the local workstation
- Restart the workstation

Site Manager application can still be used if launched via HTTPS from the network element web server. This method is immune to the Log4j vulnerability. Alternatively, the network element can be managed via the craft interfaces, including TL1 or CLI depending on functionality required.

We continue to analyze the impacts of these vulnerabilities across our other product lines and will provide updates/recommended actions as they become available.

Signature of Originator:	**CIENA Point-of-Contact**:
Ciena Global Quality Organization	Please contact your Regional Ciena Account Prime.