

Apache Log4j2 vulnerability

Update 12/17/21:

Following our vulnerability management process, Cambium Networks continues to respond to the recent vulnerabilities announced in <https://nvd.nist.gov/vuln/detail/CVE-2021-44228>. This advisory only lists Cambium Networks products and services that are known to include the impacted software component and thus may be vulnerable. Products and services that do not contain the impacted software component are not vulnerable and therefore are not listed in this advisory. Because this is an ongoing investigation, be aware that products that are currently considered not vulnerable may subsequently be considered vulnerable as additional information becomes available.

Affected Products:

At this point, we have identified that the PTP820/850 NMS system has been found to be vulnerable to Log4j. We are working diligently to get a new version available that will address the vulnerability. We will post further updates on our security page at <https://www.cambiumnetworks.com/security>. We recommend all our customers using the PTP820 product line to check back on our security page. **No vulnerabilities related to this issue have been identified on the PTP 820/850 radios themselves.**

12/13/21:

On Friday 10 December 2021, Cambium Networks became aware of a serious vulnerability in the log4j package (<https://nvd.nist.gov/vuln/detail/CVE-2021-44228>). We continue to investigate and working to patch any Cambium Networks services that use the vulnerable component. So far, we have not identified the vulnerability in cnMaestro cloud or onprem, as well as XMS-C and XMS-E. We will post further updates as more information becomes available.

Updates will also be posted to <https://www.cambiumnetworks.com/security> as additional information becomes available.