



CVE-2021-44228 (“Apache Log4j”) for LATITUDE™

Boston Scientific has reviewed the CVE-2021-44228 for the LATITUDE™ product group. See below for the outcome of that investigation:

Product	Model Number	Status
LATITUDE™ NXT	6446, 6447, 6448, 6449, 6460	Not vulnerable
LATITUDE Clarity™	7260	Not vulnerable
myLUX™ Patient App	2925	Not vulnerable
LUX-Dx™ Clinic Assistant App	2935	Not vulnerable
LATITUDE Consult™	6297	Not vulnerable
LATITUDE™ EMR Secure Courier Client	6455, 6624	Not vulnerable Vendor INFOR states product is not affected.
LATITUDE Link™	6215	Customer action needed to secure customer system. Reference the mitigation instructions below if you are using LATITUDE Link
LATITUDE™ Classic	6488	Not vulnerable
MyLATITUDE™ Patient App	N/A	Not vulnerable
LATITUDE™ Programmer & Apps	3300	Not vulnerable
ZOOM™ Programmer & Apps	3120	Not vulnerable
LATITUDE™ Communicators	6299, 6476, 6496, 6468, 6420, 6498, 6443	Not vulnerable
Heart Connect™ Tablet	3933	Not vulnerable

Visit www.bostonscientific.com/product-security for the latest official updates and additional details.

For More Information:

United States Technical Services
1.800.CARDIAC (227.3422)
tech.services@bsci.com

International Technical Services
+32 2 416 7222
intltechservice@bsci.com

Asia Pacific Technical Services
+61 2 8063 8299
aptechservice@bsci.com

For more details on the vulnerability refer to:

- [NVD - CVE-2021-44228 \(nist.gov\)](https://nvd.nist.gov/vuln/detail/CVE-2021-44228)
- [CVE - CVE-2021-44228 \(mitre.org\)](https://cve.mitre.org/cve/2021/44228/)



LATITUDE Link™ Mitigation for Apache Log4j Vulnerabilities

Technical Details

The LATITUDE Link Viewer portion of the Link application uses Log4j versions 2.11.1 and 2.13.1. A user's computer running LATITUDE Link is susceptible to the vulnerability.

To mitigate the risk this vulnerability poses, please see the mitigation options detailed below.

Mitigations

The following mitigation **prevents** a successful exploitation:

1. Please upgrade to LATITUDE Link version 1.6 if you are running an older version.
2. Navigate to the directory where the LATITUDE Link Viewer application was installed. The default location is C:\Program Files (x86)\Boston Scientific\LATITUDE Link Viewer. Do one of the following:
 - a. Replace the file named LatitudeLinkViewer.voptions with the provided patched version of the file [located here](#); or,
 - b. If your organization had previously modified the file named LatitudeLinkViewer.voptions, add the last line of the provided file to your existing version.
3. Restart the Latitude Link Viewer by either:
 - a. Restarting the computer where LATITUDE Link Viewer installed; or,
 - b. Stopping and starting the "LatitudeLinkViewer" service from the Windows Services Management Console.

The following mitigation outside of the Link application **reduces** the likelihood of a successful exploitation:

1. Please upgrade to LATITUDE Link version 1.6 if you are running an older version.
2. If the computer running the Link Viewer software is on a network that controls and whitelists outbound traffic as well as prevents inbound connections from outside the network – the Link application will not be susceptible.

Resources

If assistance is required to implement one of the above mitigations, have your IT department contact the LATITUDE EMR Support line at 888-283-8713.

Revision 1 – December xx, 2021