ICSMA-21-273-01 Boston Scientific Zoom Latitude Programmer/Recorder/Monitor Model 3120

As part of a coordinated vulnerability disclosure between academic researchers and Boston Scientific, an Industrial Control Systems Advisory has been published for the ZOOM® LATITUDE™ Programming System, Model 3120. The ZOOM LATITUDE Programming System, Model 3120, does not have network connectivity. The advisory has been published at: ICS Advisory (ICSMA-21-273-01) https://us-cert.cisa.gov/ics/advisories/icsma-21-273-01

Vulnerability Detail:

Researchers discovered the issues identified in the advisory as part of broader academic research of cardiac devices. Vulnerabilities specific to the ZOOM LATITUDE Programming System, Model 3120 include:

1. CVE-2021-38400 Use of Password Hash with Insufficient Computation Effort, CWE-916, CVSS v3 6.9
2. CVE-2021-38394 Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging techniques, CWE-1278, CVSS v3 6.2
3. CVE-2021-38392 Improper Access Control, CWE-284, CVSS v3 6.5
4. CVE-2021-38396 Missing Support for Integrity Check, CWE-353, CVSS v3 6.9
5. CVE-2021-38398 Reliance On Component That Is Not Updateable, CWE-1329. CVSS v3 6.5

For more details on the vulnerabilities, please refer to the following site:
ICS Advisory (ICSMA-21-273-01) https://us-cert.cisa.gov/ics/advisories/icsma-21-273-01

Recommendations:

Because Boston Scientific is already in the process of transitioning all users to a new, replacement programmer with enhanced security, the LATITUDE Programming System, Model 3300, we will not issue a product update to address the identified vulnerabilities in the ZOOM LATITUDE Programming System, Model 3120.

To reduce the risk of exploitation, Boston Scientific recommends following existing security measures for those still utilizing the ZOOM LATITUDE Programming System, Model 3120:

- Control access to the device and ensure all access is properly inventoried
- Maintain the device in a secure or locked location when not in use; and
- Remove protected health information (PHI) prior to retiring or removing the device from the facility. Instructions for removing PHI are outlined in the operator's manual.

Please contact Technical Services with any questions about this bulletin, precautionary measures, or any other concerns regarding our response to this matter.

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

Revision 1 – September 30, 2021