Mindray Patient Monitor Cybersecurity Brief

VS9 Username Caching

mindray
NORTH AMERICA

Intellectual Property Statement

mindray, MINDRAY and MINDRAY are the trademarks, registered or otherwise, of Mindray in China and other countries. All other trademarks that appear in this document are used only for informational or editorial purposes. They are the property of their respective owners.

Manufacturer’s Responsibility

Contents of this document are subject to change without prior notice.

All information contained in this document is believed to be correct. Mindray shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

Background

During routine penetration testing on the Mindray VS9 Vital Signs monitor a vulnerability was discovered. Usernames will be cached on a VS9 configured in Spot Check Mode with Clinician Verification using Active Directory integration or configured for Cerner VitalsLink. Cached usernames can be used to send vital signs to the EMR without having verified the user.

This vulnerability was discovered to be present in the versions of VS9 software prior to v01.13.00.01. This vulnerability does not impact VS9s not utilizing Clinician Verification in Spot Check mode or operating in Continuous mode.

The CVSS score has been determine to be 4.3 using CVSS Version 3.1; the CVSS vector string is

(AV:P/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N)

Mindray Course of Action

Mindray has released VS9 software version 01.13.00.01 which remediates this vulnerability by removing the username caching. This forces the user to be verified before patient vital signs results can be sent to the EMR.