LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

HC3: Alert
April 06, 2022 TLP: WHITE Report: 202204061200

ICS Medical Advisory - Philips Vue PACS (Update B)

Executive Summary

This updated advisory is a follow-up to the advisory update titled ICSMA-21-87-01 Philips Vue PACS (Update A) that was published January 20, 2022, to the ICS webpage on www.cisa.gov/uscert/ics. Successful exploitation of these vulnerabilities could allow an unauthorized person or process to eavesdrop, view or modify data, gain system access, perform code execution, install unauthorized software, or affect system data integrity in such a way as to negatively impact the confidentiality, integrity, or availability of the system.

Report

ICS Medical Advisory (ICSMA-21-187-01) - Philips Vue PACS (Update B)
Philips Vue PACS (Update B) | CISA

Impact to HPH Sector

In addition to following the guidance in the ICS Medical Advisory, CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA offers a range of no-cost cyber hygiene services to help organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors. All organizations should immediately report incidents to CISA at https://us-cert.cisa.gov/report, a local FBI Field Office, or U.S. Secret Service Field Office.

References

Links to additional references and resources can be found in the above referenced report.

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback