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

HC3: Sector Alert

July 8, 2021 TLP: White Report: 202107081700

Phillips Vue PACS Vulnerabilities

Executive Summary

The Philips Vue PACS (Picture Archiving and Communication System) is an image-management software platform that enables hospitals to archive, distribute, display and retrieve images and data from all hospital modalities and information systems. Vulnerabilities have been identified in Philips Vue PACS products which include 5 classified as critical that allow for a number of negative impacts including disruption, data theft and total device compromise. HC3 recommends that any healthcare organization that may operate Philips Vue PACS systems immediately confirm their inventory and review the list of recommended mitigations in this document.

Report

The Philips Vue PACS (Picture Archiving and Communication System) is an image-management software that provides scalable local and wide area PACS solutions that are widely used by hospitals, research institutions, clinics and small healthcare practices for sharing patient data and medical images. PACS technology enables hospitals to archive, distribute, display and retrieve images and data from all hospital modalities and information systems. Vulnerabilities have been identified in Philips Vue PACS products which including 5 classified as critical with a 9.8 severity rating and 4 classified high severity. Several of these vulnerabilities can be exploited remotely and are trivial to attack. Successful exploitation allows for unauthorized access, unauthorized modification of data, execution arbitrary code, eavesdropping, the installation of unauthorized software, or compromise system integrity and access to sensitive data or negatively affect the availability of the system. The vulnerabilities were recently reported by Phillips to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency who then released an alert on them. They affect the following Philips Vue PACS products:

- Vue PACS: Versions 12.2.x.x and prior
- Vue MyVue: Versions 12.2.x.x and prior
- Vue Speech: Versions 12.2.x.x and prior
- Vue Motion: Versions 12.2.1.5 and prior

Critical Vulnerabilities

CVE-2020-1938 – Improper validation of input to ensure safe and correct data processing, potentially allowing remote code execution – (CVSS 9.8/10)
CVE-2018-12326 – Buffer overflow issue in Redis third-party software allowing code execution and escalation of privileges – (CVSS 9.8/10)
CVE-2018-11218 – Memory corruption vulnerability in Redis software – (CVSS 9.8/10)
CVE-2020-4670 – Improper authentication issue within the Redis software component – (CVSS 9.8/10)
CVE-2018-8014 – Default settings for the CORS filter are not secure – (CVSS 9.8/10)

High Severity Vulnerabilities

CVE-2021-33020 – Use of a cryptographic key past its expiration date
CVE-2018-10115 – Incorrect initialization logic of RAR decoder objects in 7-Zip potentially allowing denial of service or remote execution of code via a specially crafted RAR file
CVE-2021-27501 – Failure to follow coding rule for development
CVE-2021-33022 -Transmission of sensitive/security-critical data in cleartext

Mitigations

Phillips recommends the following actions:

- Philips recommends configuring the Vue PACS environment per D00076344 –

Vue_PACS_12_Ports_Protocols_Services_Guide available on Incenter.

- Philips released Version 12.2.1.5 in June of 2020 for MyVue that remediates CWE-693
- Philips released Version 12.2.1.5 in June of 2020 for Vue Motion that remediates CWE-324
- Philips released Version 12.2.8.0 in May of 2021 for Speech that remediates CWE-693, CWE-319, CWE-119, CWE-287, and CWE-1214
- Philips released Version 12.2.8.0 in May of 2021 for PACS that remediates CWE-20, CWE-119, CWE-287
- Philips will release Version 15 in Q1 / 2022 for Speech that remediates CWE-665, CWE-327, CWE-710
- Philips will release Version 15 in Q1 / 2022 for MyVue that remediates CWE-665 and CWE-710
- Philips will release Version 15 in Q1 / 2022 for PACS that remediates CWE-79, CWE-693, CWE-665, CWE-1188, CWE-327, CWE-176, CWE-522, CWE-710, and CWE-707

DHS/CISA recommends the following actions:

- 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.

In addition to the above actions, HC3 recommends the following general security guidelines:

- Develop and maintain an IT risk management plan which should be reviewed and updated periodically, and at a minimum of 1 – 2 times per year
- Develop and maintain a comprehensive inventory of all IT systems, which should be reviewed and updated periodically, and at a minimum of 2 - 4 times per year
- Develop and maintain a vulnerability management plan in accordance with the IT risk management plan which should be reviewed and updated periodically and along with reviews/updates to the IT risk management plan; Ensure staff monitor vendor, vulnerability and government websites related to security issues with the products in their inventories

Please contact us at HC3@HHS.gov with any questions about this or any other of our products or services.

References

ICS Medical Advisory (ICSMA-21-187-01)
https://us-cert.cisa.gov/ics/advisories/icsma-21-187-01

DHS/CISA Industrial Control Systems
https://us-cert.cisa.gov/ics

Security flaws detected in Philips Vue PACS imaging equipment used in healthcare
https://industrialcyber.co/article/security-flaws-detected-in-philips-vue-pacs-imaging-equipment-used-in-healthcare/

Critical vulnerabilities in Philips Vue PACS devices could allow remote takeover
https://www.scmagazine.com/home/health-care/critical-vulnerabilities-in-philips-vue-pacs-devices-could-allow-remote-takeover/

Philips Security Advisories
https://www.philips.com/a-w/security/security-advisories.html

Philips Product Security
https://www.usa.philips.com/healthcare/about/customer-support/product-security

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