Safety Communication رسالة سلامة

May Have Cybersecurity Vulnerabilities

Device/ Product Description:	Vue PACS Systems
Affected product:	• 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
Manufacturer:	Philips Healthcare
Problem:	Philips has identified potential security vulnerabilities that under specific conditions could impact or potentially compromise patient confidentiality, system integrity, and/or system availability.
Recommendation /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. Further, Philips recommends participating in the Philips OS patching and Anti-Virus monitoring program. Philips will continue to improve cybersecurity vulnerability remediation through our Secure Development Lifecycle (SDL). Customers with questions regarding the impacted product(s) should contact their Philips support representative.

	For more information, please click here and here If you think you had a problem with your device or a device your patient uses, please report the problem to SFDA through: NCMDR Vigilance system (19999) unified call center	
Authorized Representative Details	AR name:	Philips Healthcare Saudi Arabia Ltd.
	Assigned Contact Person:	Mohammed Alsamhan
	Mobile/Phone:	0503879145
	Email:	sfda.sa.met@philips.com