HealthManagement
Promoting Management and Leadership

Critical Vulnerabilities found in GE HealthCare Ultrasound Systems

Nozomi Networks Labs has uncovered a series of 11 critical vulnerabilities in GE HealthCare's Vivid Ultrasound devices and associated software. These vulnerabilities, if left unaddressed, could potentially lead to the installation of ransomware or the manipulation of patient data. Such actions could disrupt hospital workflows and compromise data security, underlining the gravity of the situation. It's important to note that exploiting these vulnerabilities necessitates physical access to the devices, as the attacker must utilise the embedded keyboard and trackpad. GE HealthCare has responded swiftly, releasing patches and mitigations that are readily available on their Product Security Portal. Additionally, Nozomi Networks' Threat Intelligence feed has been updated to assist customers in identifying and resolving these vulnerabilities.

Vivid T9 Ultrasound System’s Comprehensive Software Suite

GE HealthCare's product line includes a diverse range of ultrasound systems, one of which is the Vivid family, specifically designed for cardiovascular care. Our research has focused on the Vivid T9 ultrasound system and its associated software, which includes the Common Service Desktop web application and EchoPAC software. The Vivid T9 is a versatile cardiac ultrasound system that also supports general imaging tasks such as vascular and abdominal exams. It operates on a customized version of Windows 10, with applications that manage most device functions. Notably, it features a restricted user interface, akin to 'kiosk' mode, which enhances its security.

The Common Service Desktop is a pre-installed web application on the Vivid T9, used for administrative tasks such as changing passwords and gathering logs. It is accessible only via the device's localhost. The EchoPAC Software Only package, installed on doctors' workstations, is used to review and analyse multi-dimensional ultrasound images. It supports data communication with the ultrasound machine by installing listeners for DICOM and SQL Anywhere DBMS communications and creating new Windows users for SMB transmissions.

Risks of Ransomware and Data Manipulation

Nozomi Networks Labs has identified several vulnerabilities in the Vivid T9 ultrasound system and EchoPAC software. These vulnerabilities, if exploited, could lead to the execution of arbitrary code with administrative privileges (NT AUTHORITY\SYSTEM) once access to the hospital environment and device is gained. This could potentially enable two primary attack scenarios, posing significant risks to the security and integrity of your operations. It's therefore imperative to apply the released patches and mitigations promptly to secure your ultrasound systems.

Ransomware: Attackers can lock the Vivid T9 or a doctor’s workstation running EchoPAC by removing Windows security protections and displaying a ransom demand on the screen. This proof-of-concept ransomware disrupts device operations.

Access and Manipulation of Patient Data: With full administrative privileges, attackers can access and manipulate all patient data stored on the devices. For EchoPAC, patient data stored in SQL Anywhere databases can be accessed and modified either by exfiltrating and loading the database files into a compatible client or by sending SQL commands to the exposed network port. The same vulnerabilities apply to the Vivid T9.

These vulnerabilities highlight significant risks to both the functionality of medical devices and the security of patient data.

General Considerations for Vulnerabilities in Healthcare

Cyberattacks targeting healthcare providers can have severe and multifaceted consequences. If a primary healthcare facility in a major city is attacked, various medical devices from different vendors, often with security vulnerabilities, could serve as entry points for broader attacks. The impacts of such an attack could include:

Inaccessibility of Medical Infrastructure: Critical procedures could be delayed, diagnoses hindered, and timely treatments impeded, affecting patient care.

Compromise of Patient Confidentiality: Breaches could lead to significant privacy violations, legal repercussions, and the misuse or sale of patient data, threatening personal privacy.

Jeopardised Diagnoses and Treatments: Disruptions could compromise the accuracy of medical diagnoses and treatment plans, potentially harming patients.

Risk managers must consider these primary consequences when assessing the impact of such incidents. GE HealthCare has conducted medical safety risk assessments, following regulatory expectations, and concluded that the associated safety risks are controlled and acceptable. These assessments, regulated by the US FDA and other bodies, require detailed evidence and trained medical staff.

The healthcare industry faces high costs and complex recovery efforts following a cyberattack. While cyber insurance is driving improvements in security infrastructure and policies, coverage in healthcare may be lower than in other industries. Healthcare providers must balance compliance, insurance, and infrastructure improvement costs against the risks and costs of an attack, recovery, and reputational damage. Maintaining privacy and confidentiality in healthcare adds complexity, making the expertise of security and risk professionals crucial for managing risk and exposure effectively.

Attack Vectors in Vivid T9 and EchoPAC Software: Physical vs. Network Exploitation

The vulnerabilities in GE HealthCare's Vivid T9 ultrasound system and EchoPAC software enable root arbitrary code execution, though the attack vectors differ. Exploiting the Vivid T9 requires physical interaction, while Echopac can be compromised over the local network.

For the Vivid T9, physical access is needed: The attack involves a two-phase process:

- Evade Kiosk Mode: Abuse the Protection Mechanism Failure issue (CVE-2020-6977) to bypass kiosk mode and gain local access.
- Command Injection: Exploit a command injection issue in the Common Service Desktop (CVE-2024-1628) to execute code with SYSTEM privileges.

This process requires operating the embedded keyboard and trackpad, but it can be expedited using a malicious USB drive that emulates keyboard and mouse actions. The attack can be completed in about one minute.

For the EchoPAC software, risk comes from network-Based Exploitation:

Local Network Access: Exploitation does not need specific credentials, only the ability to exchange network packets with the vulnerable software.

Methods of Access: This could be achieved by connecting to an internal network port, abusing an unsecured wireless network, or compromising an employee’s VPN credentials through phishing.

Both attack scenarios highlight significant risks, particularly in healthcare environments where devices might be left unattended and networks could be accessed by various means.

Mitigating Vulnerabilities: Patches and Best Practices

Asset owners can find all official patches and mitigations for the affected configurations on the GE HealthCare Product Security Portal. Nozomi Networks Labs also recommends the following additional mitigations:

- Do not leave ultrasound devices unattended, even briefly, as one minute is enough to implant malware.
- For workstations with EchoPAC installed, block incoming connections via firewall to SMB and port 2638/tcp (SQL Anywhere DB server port) when connected to an unprotected network.
- Ensure proper network segmentation and limit network communication to only essential traffic.

Source & Image Credit: NOZOMI Networks

Published on : Mon, 20 May 2024