VEDERE LABS

Internet Exposure of Medical Devices and Systems

September 26, 2022

Contents

1. Executive Summary

On September 12, the FBI released a private industry notification titled "Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities." The notification centered around a growing number of vulnerabilities in medical devices that can be exploited by threat actors to "impact healthcare facilities' operational functions, patient safety, data confidentiality, and data integrity."

This notification comes after the discovery of significant vulnerabilities this year affecting medical devices, such as infusion pumps, medication dispensing systems and electrocardiographs, as well as a wave of ransomware attacks targeting healthcare organizations in the past years, some of which have rendered medical devices unusable.

In this report, we discuss why medical devices are vulnerable, go beyond vulnerabilities to provide a picture of the exposure of medical devices and systems on the open internet and discuss mitigation recommendations for healthcare organizations.

Key findings of this report include:

- We identified more than 7,000 exposed medical systems on the internet, including PACS, healthcare integration engines, EMR, medication dispensing systems and others. Some medical devices, such as medical image printers, are also directly exposed.
- The United States has the vast majority of these exposed systems (58% of the total), followed by Iran, India and Brazil.
- Almost half of the exposed systems are PACS, which typically rely on the DICOM protocol for medical imaging storage and retrieval. Looking specifically at DICOM systems, we observe 4,114 exposed systems, an increase of 14% over a year ago.
- Applying effective network segmentation is the most important mitigation action considering our findings about exposed systems.

2. Why are Medical Devices Vulnerable?

The FBI notification cites four common issues that lead to vulnerabilities being found or remaining unpatched in medical devices. We have previously explored all those issues in different research projects.

- **Devices used with a default configuration are easily exploitable.** Many medical devices have default open ports or credentials when they are configured by a manufacturer, and sometimes these are not changed when deployed in healthcare organizations. In our Access:7 research, we identified medical devices that were shipped with a configuration agent still present and whole product lines sharing hardcoded credentials for remote access.

- **The long lifespan of medical devices allows threat actors ample time to find and exploit vulnerabilities.** Medical devices are used in organizations for 10 to 30 years, which not only gives time to find vulnerabilities, but also the code running on them is potentially decades old. In our NUCLEUS:13 research, we found vulnerabilities on a software component used in medical devices since 1993.

- **Devices require special upgrading procedures that delay patching.** Due to specialized software and firmware running on many medical devices, the patching procedure is not as easy as in a traditional computer. Not only is applying patches is more difficult, but even the existence of patches is not guaranteed for vulnerabilities affecting third-party components. This is an issue we discussed at length during our Project Memoria research.

- **Devices were not designed with security in mind.** Many of the protocols running on these devices do not include basic security controls such as authentication and encryption. We have recently discussed the issue of insecurity by design in operational technology as part of OT:ICEFALL, but we also have demonstrated in the past how insecure protocols in healthcare allow attackers to leak patient data, tamper with diagnostic results, disconnect a patient monitor and even change a patient's vital readings on the network.

One of the main reasons for the persistent insecurity of medical devices is the belief that those devices are not exposed to cyberattacks because they can only be accessed from inside a hospital's privileged network. The fact that many remote ransomware attacks have spilled over to medical devices and related information systems is proof enough this assumption is no longer true. Beyond reported attacks, we have shown persistent segmentation issues in healthcare organizations, where several unrelated types of devices with very different criticality levels are present in the same network segments, providing a path for attackers to reach medical devices.

The truth is that medical devices often are not connected directly to the internet, but they communicate with information systems that are exposed online. For instance, imaging modalities, such as CT scanners, communicate with picture archiving and communication systems (PACS), which in turn communicate with radiology information systems (RIS). Although CT scanners are not found online, many PACS and some RIS are and thus may provide a path for attackers to reach the most sensitive devices.

3. An Analysis of Internet-exposed Medical Systems

Using a series of specific network fingerprints of medical systems (openly accessible to anyone, including attackers), we queried the Shodan search engine and found a total of 7,168 exposed systems. These systems have the following distribution per country.

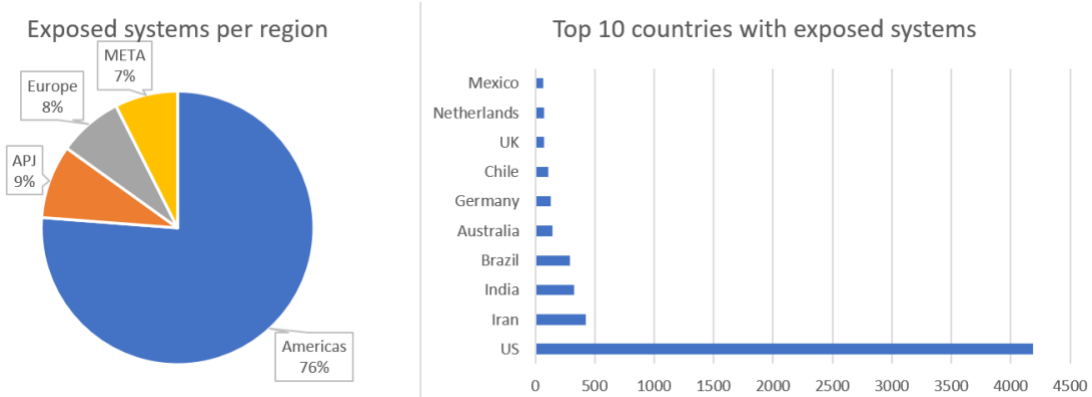


Figure 1 – Distribution of exposed medical systems per country

More than three quarters of systems are in the Americas, with the United States alone having 4,185 (58% of the total). The Asia-Pacific and Japan (APJ) region comes second, mainly represented by India (324 exposed systems) and Australia (146). Europe comes third as a region, with the majority of exposed systems in Germany (128), the United Kingdom (75) and the Netherlands (71). Finally, in the META region (Middle East, Turkey and Africa), the most representative country is Iran, with 427 exposed systems.

The exposed systems are divided into the following types.

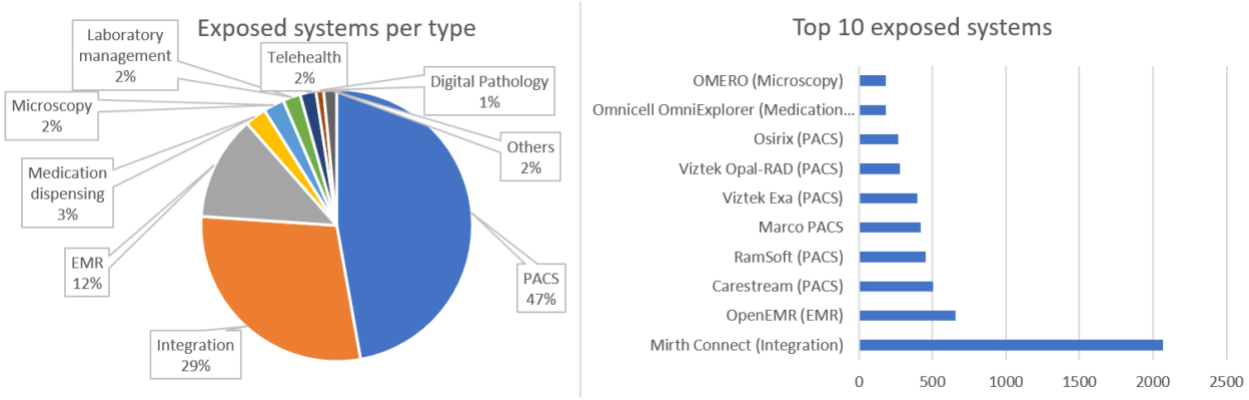


Figure 2 – Distribution of exposed medical systems per type

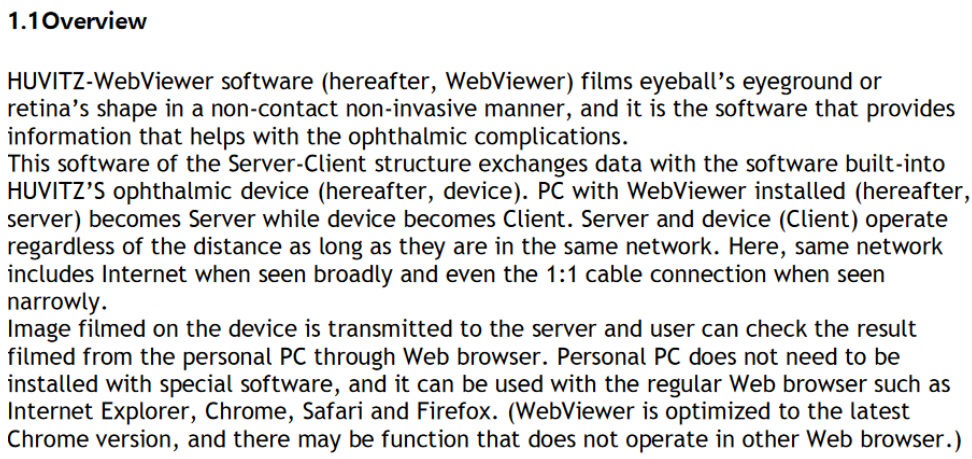
Almost half of them are PACS, used for the storage and visualization of medical images relying on the standard DICOM protocol. The second most popular category is healthcare integration engines used to standardize data flows across separate systems, such as clinical, financial and operational data. These engines often use the standard HL7 protocol. The third category is electronic medical records (EMR) systems used to manage patients' health data. One interesting and surprising category in the top 10 is medication dispensing systems, typically used in hospital pharmacies.

The "Others" category in Figure 2 includes things such as decision support systems, radiology information systems, patient management systems and two interesting findings:

- Agfa DryStar printers for medical images, with a welcome screen shown in the image below. This finding exemplifies direct access to medical devices and not only information systems.

Figure 3 - Screenshot of an exposed medical image printer

- Huvitz HOCT-1F WebViewer systems to manage optical coherence tomography (OCT) devices. The manual of this device exemplifies the type of access that these exposed systems provide and how they are connected directly to medical devices, as shown in Figure 4 below.

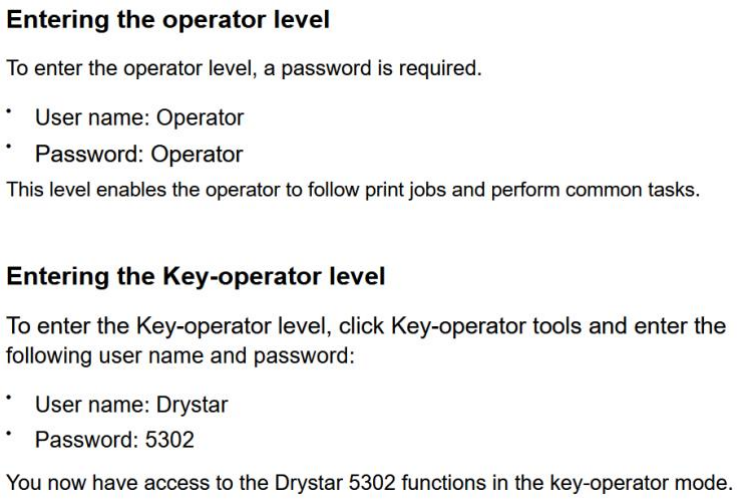


1.1 Overview

HUVITZ-WebViewer software (hereafter, WebViewer) films eyeball's eyeground or retina's shape in a non-contact non-invasive manner, and it is the software that provides information that helps with the ophthalmic complications.
This software of the Server-Client structure exchanges data with the software built-into HUVITZ'S ophthalmic device (hereafter, device). PC with WebViewer installed (hereafter, server) becomes Server while device becomes Client. Server and device (Client) operate regardless of the distance as long as they are in the same network. Here, same network includes Internet when seen broadly and even the 1:1 cable connection when seen narrowly.
Image filmed on the device is transmitted to the server and user can check the result filmed from the personal PC through Web browser. Personal PC does not need to be installed with special software, and it can be used with the regular Web browser such as Internet Explorer, Chrome, Safari and Firefox. (WebViewer is optimized to the latest Chrome version, and there may be function that does not operate in other Web browser.)

Figure 4 - Snippet from Huvitz WebViewer manual

Both devices shown above have login screens, but they also have default passwords described in their manuals, as shown in Figure 5 below for the DryStar printers. For ethical reasons, we did not test any of the passwords on the exposed devices we found.



Entering the operator level

To enter the operator level, a password is required.

- User name: Operator
- Password: Operator

This level enables the operator to follow print jobs and perform common tasks.

Entering the Key-operator level

To enter the Key-operator level, click Key-operator tools and enter the following user name and password:

- User name: Drystar
- Password: 5302

You now have access to the Drystar 5302 functions in the key-operator mode.

Figure 5 - Snippet of the Agfa DryStar printer manual with default passwords

Looking only at the top 10 exposed systems, we found that 882 out of 5405 (16%) had at least one vulnerability identified by Shodan. For some systems, the vulnerability rate was much higher. For Opal-RAD PACS it is 69%, for Carestream PACS it is 50% and for OpenEMR, it is 31%. It also is important to notice that many other systems could have vulnerabilities that are not automatically identified by the search engine.

Since PACS are the most common type of exposed system, we decided to take a closer look at them. As mentioned above, PACS systems typically use the DICOM protocol, so we can extended our search to find more exposed systems using the query "DICOM Server Response" which returns 4,114 new results (825 of which are identified as honeypots to attract attackers, since there exists popular open honeypots for DICOM). Interestingly, we can also see an upward trend of exposed devices using DICOM.

Figure 6 - Upward trend of exposed PACS running DICOM

These DICOM systems are present in the following countries. Again, the United States comes first with more than 1,000 exposed systems.

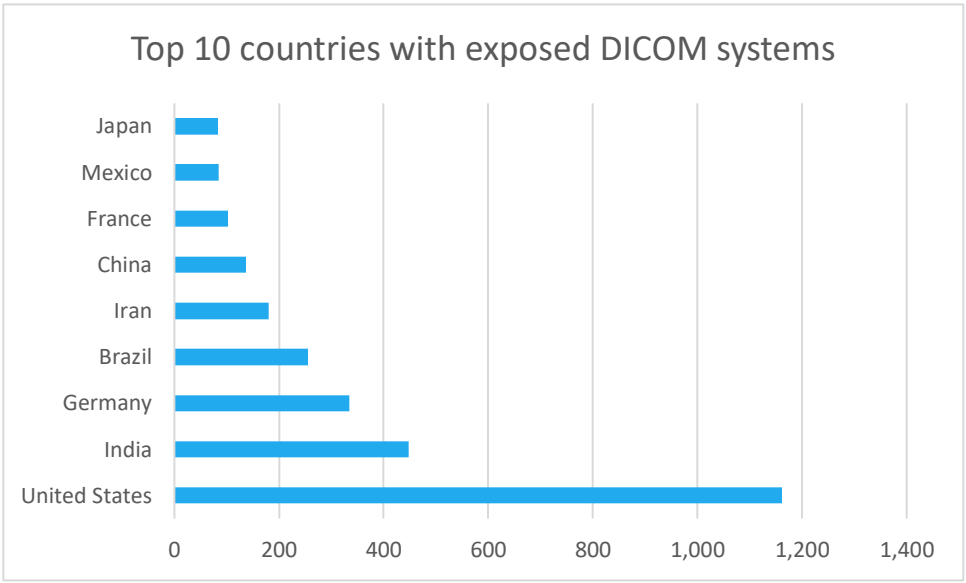


Figure 7 - Distribution of exposed DICOM systems per country

Devices using DICOM expose the name (or an identifier) of the server application on the banner grabbed by Shodan. One of the most popular servers found online uses the OFFIS DICOM Toolkit, which had a set of vulnerabilities disclosed as recently as June.

4. Mitigation Recommendations

The FBI notification proposes five categories of mitigation actions for vulnerable medical devices:

- Run endpoint protection, such as antivirus and EDR, on devices that support those technologies.
- Use complex unique passwords per device and limit the number of login attempts.
- Maintain an inventory of medical devices and use it for risk assessment.
- Follow security advisories from vendors and run vulnerability scanning on medical devices.
- Implement security training for employees to identify and report problems such as insider threats, phishing and social engineering.

The notification also encourages to “take other mitigation precautions, such as isolating the device from network or auditing the device’s network activities.” For more detailed guidelines on implementing segmentation for specific device types, such as PACS, EMR and infusion pumps, see NIST’s security guidance publications. For general guidance on risk assessment of medical devices, see the recent NIST SP 800-66.

Network segmentation is extremely important considering our findings about exposed systems. The FBI’s recommendations, particularly segmentation and network monitoring, should apply not only to medical devices but also to every device on your organization’s network. As we showed in previous posts and as the Health Sector Cybersecurity Coordination Center (HC3) discussed recently, threat actors can leverage those other types of devices to gain access to or impact healthcare organizations.