MEDIGATE

Top Healthcare Cybersecurity Threats of 2021

As 2021 comes to a close, we at Medigate took a look back at what happened this year in healthcare security. Now, it would've been considerate for the "bad guys" to take a break and give our healthcare delivery organizations (HDOs) time to focus on the global pandemic. Unfortunately, they continued to attack.

The Medigate Data Team compiled a list of the most severe vulnerabilities and attacks in the healthcare sector. While this review is certainly not exhaustive, it highlights the sheer volume of attacks on medical devices and the most critical issues of 2021 (besides the global pandemic).

Today's healthcare environment is expanding as connected medical devices are expected to grow an additional 42% by 2025. These devices improve patient care, so the growth corresponds with improving healthcare outcomes. However, more devices mean more attack surfaces that must be secured to avoid compromises or disruptions to patient care.

Attacks are rising, with many estimates placing the 2021 increase at around 40%. Medical devices are a common attack vector, and securing them requires diligence and skill. While each episode has its own unique characteristics, there are similarities between the attack types – attacks to medical devices that have come through IoMT vulnerabilities, platform vulnerabilities, and third-party access.

This report highlights the top offenders in each of these vectors and provides some generalized recommendations to secure your network. While no one can predict the future exactly, we can confidently expect the trend of bad actors attacking healthcare cyber-physical systems to continue increasing next year. This report looks at those trends and concludes with some general thoughts about the state of device security in 2022.

How we got our findings

The observations shared below originate from the real-world data of Medigate's customers and partners, which include more than 10 million devices (1 million unique device types) across 100+ HDOs and over 1000 individual hospitals. Medigate Research Labs discovered and then reported two of the threats covered in the report to the vendor and user community as part of our commitment to advancing the healthcare market's cybersecurity research and data integrity. Overall, Medigate Research Labs saw a notable expansion of medical devices as they tracked known and emerging threats. The Medigate Data team observed the following:

14.5%

Growth of connected medical devices.

30%

Devices are potentially affected by two or more critical vulnerabilities.

20%

Medical devices shouldenroll in an MDM tool, but only 7% of the eligible pool are.

As noted, 2021 was a doozy of a year. Fortunately, with trained cybersecurity people, detailed processes, and appropriate technology, HDOs can address the growing number of threats they are facing. The goal is to prevent the successful exploitation of vulnerabilities and attack vectors that can impact multiple device types, impair patient treatment, and put lives at risk.

1. IoMT Vulnerabilities

Specific vulnerabilities that target unique devices show how organized and motivated the attackers are. Targeting specialized instruments requires dedication and skill on the part of the bad actor. Still, the potential financial payoff is worth it since these devices connect to patients and their information. The willingness and ability to patch specific devices are dependent on many factors, and some may have no reasonable remediation steps available anytime soon. Understanding the overall risk of particular devices, as opposed to generalized device classes, will become a significant theme for healthcare security teams going forward.

B. Braun Infusion Pumps - ICSMA-21-294-01 (August 2021)

In August, McAfee announced the identification of five vulnerabilities in two widely used models of B. Braun drug infusion pumps. These devices are used globally in hospitals to treat patients and automate the delivery of medication and nutrients that's especially useful for delivering critical and life-sustaining medicines. Remote attackers could exploit these vulnerabilities to change the device's configuration, resulting in an incorrect dosage of medication and potentially causing harm to a patient. Attackers could also use the threat of this attack to force a ransom payment by an HDO.

Specifically affected models:

- Battery Pack SP with WiFi
- SpaceStation with SpaceCom 2

How to Protect Your Network

- **Patch Affected Devices:** B. Braun released software updates for the affected devices. Medigate recommends physically locating all affected devices in your environment and applying the software patch.

- **Network Segmentation:** Where physical location and remediation are not possible, the best practice is to apply proper network segmentation to mitigate the risk.

Welch Allyn (HillRom) - ICSMA-21-152-01 (June 2021)

In June, Medigate Research Labs discovered and reported Out-of-Bounds Write and Read vulnerabilities in Welch Allyn monitors and medical device management tools. Medical teams use these devices to monitor blood pressure, pulse rate, and body temperature and notify them immediately about cardiac arrhythmias at the bedside.

Successful exploitation of those vulnerabilities could allow an attacker to cause memory corruption and remotely execute arbitrary code, compromising the integrity of the device and potentially affecting the treatment of patients. This attack could also be used as a threat to force a ransom payment from an HDO.

How to Protect Your Network

- **Patch Affected Devices:** Welch-Allyn released software updates for the affected devices. Medigate recommends physically locating all affected devices in your environment and applying the software patch.
- **Network Segmentation:** Where physical location and remediation are not possible, the best practice is to apply proper network segmentation to mitigate the risk.

2. Platform Vulnerabilities

Commonly used software platforms were a popular source of vulnerability in 2021. Bad actors can affect broad swaths of devices that rely on it for operation by disrupting an underlying software stack. These platforms will generally have software patches available, but understanding which devices use the operating system can be challenging, causing many devices to miss critical updates and patches each year.

Log4Shell - Apache Log4j Vulnerabilities (December 2021)

On December 9th, an exploited-in-the-wild Log4Shell vulnerability, tracked as CVE-2021-44228, was disclosed in Apache Log4j versions 2.0 to 2.14.1, throwing the IT world into a panic. Log4Shell carries a CVSS score of 10 out of 10 and threatens popular consumer and enterprise applications, cloud services, and websites that use the open-source logging library, Apache Log4j.

This has caused all vendors to evaluate their products and determine which is vulnerable, underscoring the need for a Software Bill of Materials (SBOM) to understand exposure.

Since the initial discovery, several more vulnerabilities have been disclosed in additional versions of log4j, including log4j 1.x and the patches for the CVE-2021-44228 vulnerability.

Many common medical device software applications are impacted. In light of this, Log4Shell has become one of the most significant concerns for HDOs in 2021. Please refer to our blog, which is continuously updated as more devices are identified, for more information.

How to Protect Your Network

- **Identify & Locate Affected Devices:** As more device manufacturers release information about their usage of Log4Shell, locating the impacted devices will be a high priority. We recommend focusing on Internet-facing endpoints.

- **Patch Affected Devices:** Ensure that all patches are applied when released. The most effective protection will be to upgrade to log4j-2.17.0 as soon as possible.

- **Network Segmentation:** Medigate also recommends enforcing segmentation controls and proper network hygiene to mitigate the risk from vulnerable devices. Restrict Internet communication where it is not necessary for the intended use.

- **Vulnerability Scanners:** A key tool that can be used is your vulnerability management solution. Using Medigate Clinical Cyber Hygiene, you can create a targeted scan of all potentially vulnerable devices and scan those at once. This will enable you to map all vulnerable devices based on a combination of passive and active information.

- **Monitor Network Traffic & Device Behavior:** Use Medigate's communication alerts to determine whether the devices in your environment communicate with malicious IPs associated with Log4j attacks. For a full list of IoC associated with Log4j attacks, see this link.

NUCLEUS:13 - Nucleus TCP/IP Stack (November 2021)

In November, Medigate Research Labs and Forescout Research discovered a set of 13 new vulnerabilities affecting the Nucleus TCP/IP stack, collectively known as NUCLEUS:13. Of these vulnerabilities, these 6 CVEs are the ones with the most critical CVSS scores:

CVE-2021-31890	CVE-2021-31346	CVE-2021-31345
CVE-2021-31889	CVE-2021-31884	CVE-2021-31886

Nucleus NET is the TCP/IP stack of the Nucleus Real-Time Operating System (RTOS), owned by Siemens. It has been deployed in many industry verticals with safety and security requirements. This vulnerability affects medical devices such as Anesthesia Machines, Patient Monitors, and C-Arms within healthcare.

Successful exploitation of these vulnerabilities could result in remote code execution, denial-of-service attacks, and information leakage.

How to Protect Your Network

- **Identify & Locate Affected Devices:** With the broad distribution of this RTOS, it is crucial to determine which devices in your network rely on this operating system and then prioritize the ones with the highest risk. Because so many devices are affected, we recommend beginning with devices with a Common Vulnerability Scoring System (CVSS) score of 9.8 or higher.
- **Patch Affected Devices:** Complete protection against NUCLEUS:13 requires patching. Siemens has released a software patch, and HDOs should update impacted devices immediately.
- **Network Segmentation:** Medigate recommends enforcing segmentation controls and proper network hygiene to mitigate the risk from vulnerable devices.

BadAlloc - Real-Time Operating Systems (April 2021)

In April, Microsoft discovered 25 vulnerabilities, collectively named “BadAlloc,” found in multiple RTOS’s and supporting libraries, including QNX, VxWorks, and MQX.

The widespread use of these operating systems in medical devices means the vulnerabilities could potentially affect thousands of products, such as C-Arms, Immunoassay Analyzers, Robotic Surgery Systems, Infusion Pumps, and Nurse Call systems.

Six of the vulnerabilities are rated “Critical,” with a CVSS score of 9.8 because remote attackers can exploit those vulnerabilities with little complexity. According to the Cybersecurity & Infrastructure Security Agency (CISA), successfully exploiting these vulnerabilities could result in unexpected behavior, such as a crash or a remote code injection/execution.

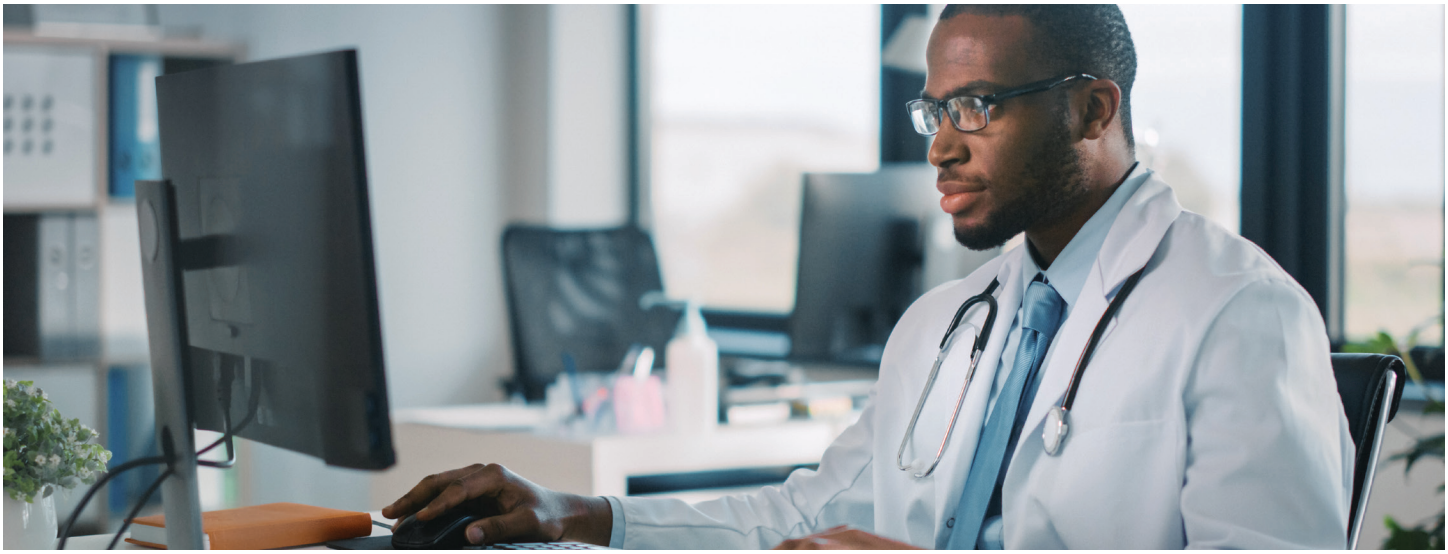
CVE-2021-31571	CVE-2021-31572	CVE-2020-35198
CVE-2021-3420	CVE-2021-26461	CVE-2021-22156

The above medical devices play a crucial role in the healthcare ecosystem, and any interruption could impede care delivery.

CISA urges organizations with vulnerable devices to apply patches where possible. In addition to minimizing the network exposure for the potentially vulnerable medical devices, Medigate recommends using vetted segmentation policies.

How to Protect Your Network

- **Prioritize the Critical Vulnerabilities:** With the broad distribution of this RTOS, it is crucial to determine which devices **on** your network rely on this operating system and prioritize the ones with the highest risk.
- **Patch Affected Devices:** There are some patches released for these devices. Physically locate all affected devices in your environment and apply the correct software patch to ensure remediation.
- **Network Segmentation:** Where physical location and remediation are not possible, the best practice is to apply proper network segmentation to mitigate the risk from vulnerable devices.



PrintNightmare (July 2021)

In July, Microsoft disclosed two vulnerabilities affecting the Windows Print Spooler service. If successful, the Microsoft Windows Print Spooler service fails to restrict access to add printers and related drivers, allowing a remote authenticated attacker to execute arbitrary code with SYSTEM privileges on a vulnerable system.

These risks are particularly concerning because the service is enabled by default for some devices. The vulnerabilities are in all versions of Windows Server and Windows 7, 8, and 10.

Many security researchers wrote about the impact of this vulnerability. Microsoft and the CISA recommend applying updates or using one of the listed workarounds.

How to Protect Your Network

- **Patch Affected Devices:** There are some patches released for these devices. Physically locate all affected devices in your environment and apply the patch to ensure remediation.
- **Network Segmentation:** Where physical location and remediation are not possible, the best practice is to apply proper network segmentation to mitigate the risk from vulnerable devices.
- **Workaround:** There are some acceptable workarounds if patching and segmentation are impossible. Investigate which is correct for your devices and determine if the workaround is feasible.

3. Third-Party Access

In the past year, the phenomenon of threat actors using third-party business associates as entry points into customer networks continued to increase.

This threat poses a significant risk for healthcare systems, which are increasingly outsourcing core functions and contracting third-party vendors to perform essential operations in their environment.

With this type of attack, ransomware is inserted into a third-party business network, which an attacker can then use to get into the HDO environments that the business is servicing. This means, instead of attacking the HDO directly, they can impact a broad set of them, compromising a mutual vendor to attack and potentially damage many organizations.

Two incidents from the past year underscored the potential severity of this risk:

Elekta (April 2021)

On April 6, 2021, **Elekta**, a provider of radiation therapy equipment, was hit by a ransomware attack on their cloud-based systems. According to their spokesperson, the "...issue was only isolated to a subset of US Cloud Customers due to [their] Geographical and Service Segmentation in Cloud Services. No other Elekta servers, services, or products [were] affected. Additionally, there is no evidence that any data was extracted or copied."

Following the attack, Elekta was forced to take its cloud-based storage system offline to contain the breach after the attack. As a result, a subset of customers in the U.S. canceled or rescheduled some radiation treatment appointments.

MEDIGATE

Olympus (October 2021)

Olympus, a manufacturer of optics and reprography products, was forced to take down IT systems in the Americas (U.S., Canada, and Latin America) following an attack that hit its network on Oct. 10, 2021. This incident follows a ransomware attack that hit the company in September and disrupted EMEA operations.

Olympus confirmed that the attack did cause temporary disruptions to business operations, but they didn't disclose whether attackers accessed customer data during the cyberattack. They have promised to provide more information when it becomes available.

How to Protect Your Network

- **Proper Third-Party Vetting:** Review all third parties who have access to the clinical network to ensure compliance with security best practices. Conduct standardized security assessments and calculate the blast radius from any potential service disruptions.
- **Network Monitoring:** Use tools to monitor network traffic and device behavior to provide early warning about Indicators of Compromise (IoCs).
- **Network Segmentation:** Medigate recommends clinical and context-based network segmentation to ensure potentially affected devices are quickly isolated.

Our Predictions for 2022

Unlike shaking a 'Magic 8 Ball', predicting the future of healthcare security is not easy. While we look deeply into the current trends—such as our recently published research with CrowdStrike on the state of ransomware—continuing to stay ahead of emerging threats requires diligence, excellence, and creativity.

These trends indicate that attacks will continue to increase in velocity and complexity. Bad actors will focus on identifying weak points in cyber-physical security and have no qualms about using any gaps to shut down the delivery of care from an HDO to their patients and extorting a ransom.

In 2022, a few trends will continue, forcing HDOs to respond in novel ways:

1. An HDO may be found liable for an adverse patient outcome attributed to a ransomware attack. Any resulting civil penalty could be a significant and potentially precedent-setting damage award.

2. The cyber-insurance marketplace will continue to mature, and carriers will ask more and better questions of their HDO clients to justify the coverage and manage the risk. Additionally, the cost of cybersecurity insurance will continue to increase rapidly.

3. With the cost of cyber insurance on the rise, HDOs may try to get by with less coverage and assume more of the risk their cyber insurer has traditionally borne. This adjustment will spur radically different investments in cybersecurity people, processes, and technology.

4. HDOs will begin to earnestly look at “As A Service” models for risk management - either delivered by their cyber insurance carriers or trusted third-party partners. The main thing HDOs will be looking for is additional capabilities or expertise to augment their existing teams.

By and large, the best response will be to improve the situational cyber-physical risk awareness of HDOs. Based on these predictions, accurate information about the connections, devices, and users will enable better network architecture, segmentation, and security decisions. With a complete understanding of what is connecting, health organizations can make informed decisions about risk and better leverage the tools available from cyber insurance carriers and trusted third parties.

For More Information

Thank you for reading our retrospective of the worst healthcare cybersecurity threats in 2021. Amid a crazy year full of surprises and challenges, these threats were indeed forces to be reckoned with. As the number of attacks continues to climb, you can count on Medigate to support you with accurate data regarding your clinical devices and their known threats.

To learn more about Medigate Research Labs and the Threat Intel Feed, please visit www.medigate.io/threat.

MEDIGATE

Email: **contact@medigate.io**
Visit: **medigate.io**