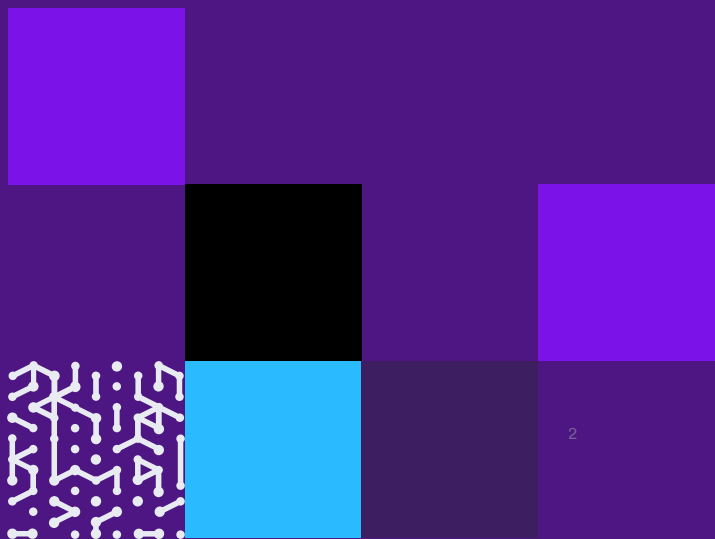
ARMIS LABS INSIGHTS

Q4, 2024

Early Warning Insights to Protect Healthcare Systems

Focus on the Most Critical Risks Before They Impact Your Environment



Executive Summary

Take a Proactive Approach

This report provides healthcare organizations with key insights to proactively address cybersecurity threats and vulnerabilities, and prioritize the mitigation efforts against relevant threat actors in the healthcare industry.

For CISOs, the report offers an overview of current risks, widely exploited vulnerabilities, and emerging threats. For Vulnerability Management- and broader Security teams, it offers a practical list of CVEs, TTPs (Tactics, Techniques, and Procedures) and IOCs (Indicators of Compromise) for organizations to address and monitor.

Key Takeaways

Advanced Persistent Threat (APT) Groups

We identified the top 3 APT groups actively targeting healthcare, including APT41 (China), APT37 (North Korea), and APT20 (China). Understanding their tactics, techniques, and procedures (TTPs) is crucial for a proactive defense.

Early Warning Spotlights

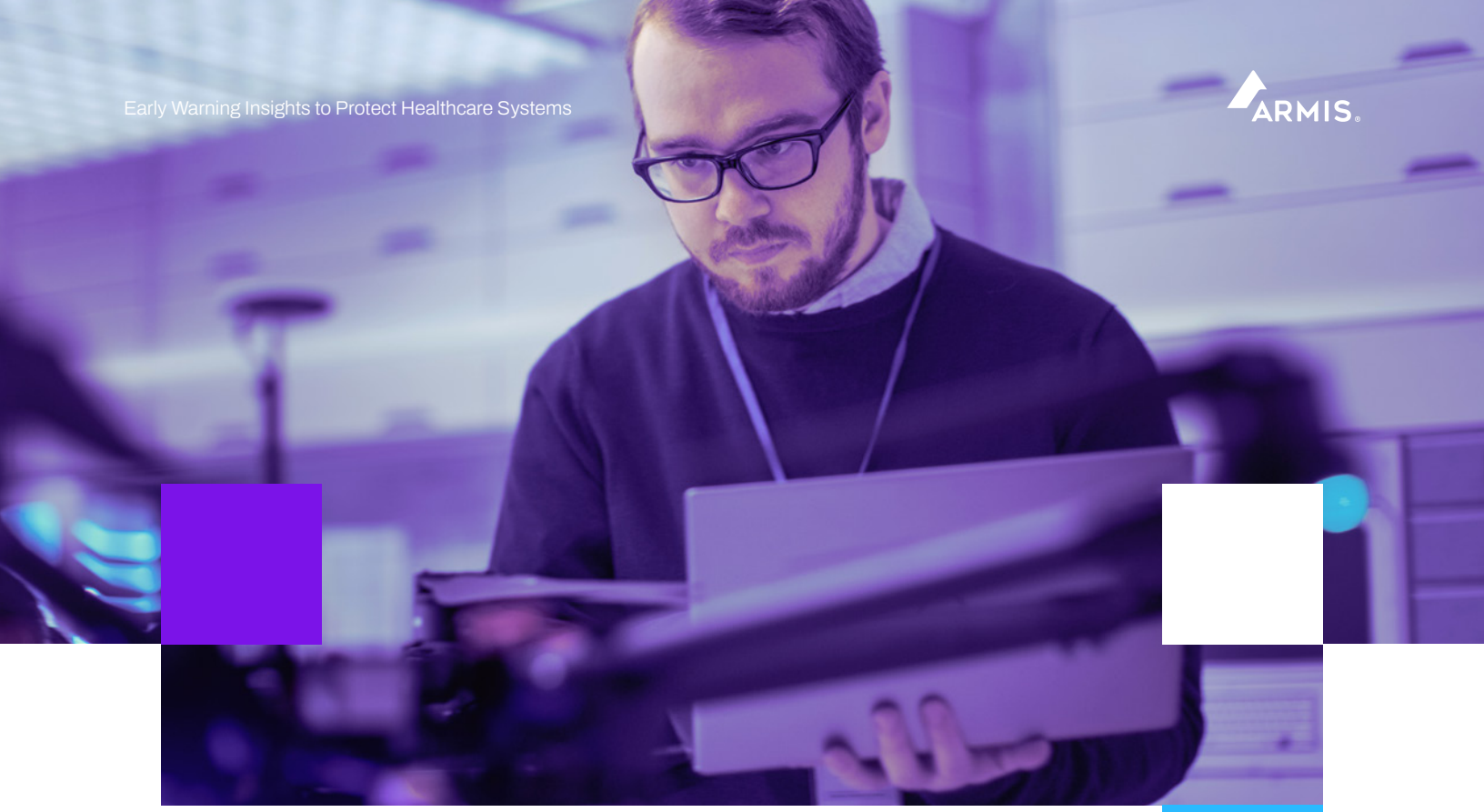
We highlighted two critical vulnerabilities (CVE-2023-43208 and CVE-2024-39891) impacting Electronic Health Records (EHR) systems and Telehealth solutions. Armis Labs provides actionable insights to mitigate these risks as well as the scope of impacted organizations within the Armis Asset Intelligence Engine.

High-Impact Ransomware Groups

We profiled the most active ransomware groups targeting healthcare, including LockBit 3.0, ALPHV (BlackCat), and BianLian. The report details their attack methods and provides recommendations for bolstering defenses.

Emerging Threats

Armis Labs identifies widely exploited and emerging CVEs in healthcare environments, offering proactive guidance for vulnerability management.



Top 3 Advanced Persistent Threat (APT) Groups

Advanced Persistent Threat (APT) groups are cyberattack entities, typically nation-states or state-sponsored organizations that use sophisticated hacking methods to achieve specific objectives. Unlike generic malware campaigns, APT attacks are “persistent,” meaning they often maintain access to their targets over long periods, silently collecting data or infiltrating further into networks.

> **APT groups utilize cutting-edge tools, techniques, and intelligence to evade detection and exploit vulnerabilities. Their primary goal is to establish long-term access to a target’s systems, enabling consistent data exfiltration or surveillance. Many APTs are backed by substantial funding and resources, often provided by governments or large criminal organizations.**

These characteristics make APT groups one of the most challenging threats for security professionals to defend against. Their campaigns can take months or even years to fully unfold, frequently avoiding detection until it’s too late. At Armis Labs we use cutting-edge technologies, including dynamic honeypots, incident forensics, reverse engineering, dark web monitoring, and human intelligence, to proactively identify threats and dangerous trends before they manifest. Armis Labs can help you stay ahead of cyber adversaries, and proactively protect your organization before the threat arrives at your doorstep.

Here's an overview of what Armis Labs believes are the current top 3 APT Groups to watch as they have shown direct interest in the healthcare industry recently, along with their TTPs (Tactics, Techniques, and Procedures) and IOCs (Indicators of Compromise):

APT41

Attribution	China
Sectors	Healthcare, telecom, and hightech
Overview	APT41 is known for both the purpose of espionage and financially motivated activities. It has targeted healthcare for intellectual property theft and data collection, sometimes overlapping state and nonstate interests.
TTPs	• Spear phishing emails with malicious attachments (e.g., compiled HTML files) • Use of rootkits and Master Boot Record (MBR) bootkits for persistence • Deployment of a wide array of malware, including credential stealers, backdoors, and keyloggers
IOCs	• Associated malware: 46+ code families including custom backdoors • Evidence of compromised systems across healthcare organizations globally

APT37

Attribution	North Korea
Sectors	Healthcare, chemicals, manufacturing, and more
Overview	Conducts cyber espionage operations aligned with North Korean state interests. Known for leveraging zeroday vulnerabilities
TTPs	• Social engineering tailored to healthcare professionals • Exploitation of software vulnerabilities (e.g., Hangul Word Processor and Adobe Flash). • Deployment of custom espionage and destructive malware
IOCs	• Malware variants with exfiltration capabilities. • Use of zeroday vulnerabilities like CVE-2018-0802

APT20

Attribution	China
Sectors	Healthcare, construction, nonprofits, defense, and chemical
Overview	Primarily focuses on data theft and monitoring politically sensitive activities and organizations
TTPs	• Strategic web compromises targeting healthcare professionals and entities • Phishing lures related to healthcare themes • Deployment of known malware families like QIAC and SOGU
IOCs	• Malware families used include Gh0st, ZXSHELL, and BEACON. • Exploited vulnerable web servers within the healthcare domain

Early Warning Spotlights

Though your organization may have taken a proactive approach to managing vulnerabilities, your teams are likely overwhelmed by the millions of alerts coming from new security tools, and may struggle to automate prioritization based on context and risks specific to their environment. To combat this, Armis Centrix™ for Early Warning combines **asset intelligence** with **vulnerability intelligence**.

Asset intelligence provides a complete inventory of the healthcare industry internal environment, like a detailed map of the attack surface across all of Armis customers in the industry. Our vulnerability intelligence uses SOTA techniques to see what vulnerabilities and TTPs threat actors are using in the wild or about to weaponize.

Combining these methods allows CISOs to:

Prioritize vulnerabilities

Focus on those posing the greatest risk to your specific attack surface.

Reduce alert fatigue

Address the most critical alerts based on potential impact.

Optimize resources

Protect the most valuable and vulnerable assets.

Proactively mitigate risks

Anticipate and defend against attacks based on attacker behavior and known vulnerabilities.

Asset intelligence shows you “what needs protecting,” while vulnerability intelligence reveals “what’s coming to attack it.” This empowers proactive, risk-based cybersecurity.

Early Warning empowers you with actionable intelligence before an attack is launched and before your organization is impacted.

Early warning vulnerability intelligence can detect and neutralize malicious actions in your environment before they are exploited. Having robust visibility, protection, and alerts management in place can provide an effective threat forecast and a realistic picture of where to focus your efforts.

For this report, Armis Labs put together a selection of 2 specific Healthcare Early Warning Spotlights based on a rigorous assessment that goes beyond just vulnerability prioritization. Factors considered include:

Threat Actors Intent: The motivation of threat actors to focus on the relevant vulnerability or access.

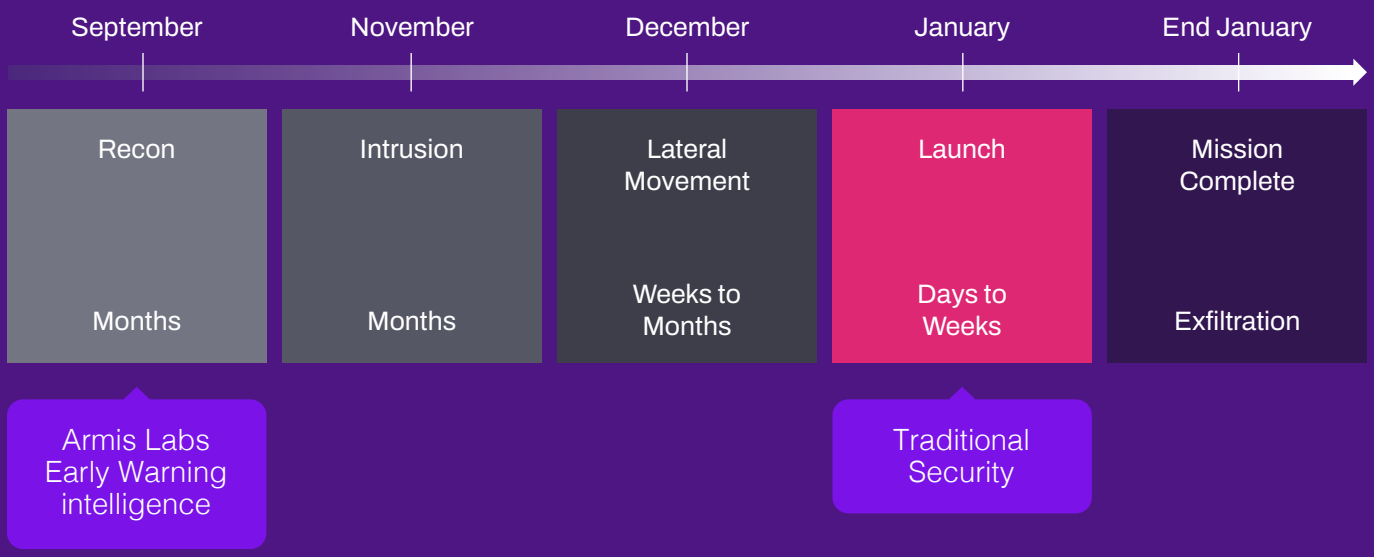
Exploit Maturity: Prioritizing vulnerabilities with known functional exploits available in the wild, indicating immediate and significant risk.

Impact Severity: Focusing on vulnerabilities that could lead to critical impacts like remote code execution, data breaches, or system compromise.

Asset Criticality: Evaluating the potential impact on critical systems and infrastructure within your organization.

Vulnerability Prevalence: Considering how widespread the vulnerability is within your environment, prioritizing those affecting a larger number of assets.

Mitigation Availability: Assessing the availability of patches, workarounds, or mitigation strategies to address the vulnerabilities effectively.



Ordinary security goes to work when an attack is launched. Armis Labs early warning intelligence finds potential threats before they are ever launched and before your environment is ever impacted. In many cases, months early.

This multi-faceted approach ensures that the “spotlight” shines on the most urgent and impactful threats, enabling efficient resource allocation and maximized risk reduction. This targeted “spotlight” strategy allows for:

Rapid Response: Concentrated efforts on patching or mitigating these 2 vulnerabilities minimizes your attack surface against active threats.

Resource Optimization: Devoting resources to validated, high-impact threats avoids spreading your security team too thin.

Reduced Dwell Time: Faster patching cycles for critical vulnerabilities limit the window of opportunity for attackers.

Improved Communication: A concise spotlight facilitates clear communication to stakeholders about imminent threats and remediation efforts.

Data-Driven Defense: This process leverages threat intelligence to guide security decisions, enhancing your overall security posture.

By focusing on 2 high-confidence early warnings of in-the-wild exploits, you’re prioritizing the most critical threats to your organization.

Spotlight 1

Electronic Health Records (EHR) Systems

CVE-2023-43208

First Exploit Publish Date
Oct 24, 2023

CISA Due Date
Jun 9, 2024

16 **Number of Exploits**

Electronic Health Records (EHR) systems have revolutionized healthcare, streamlining operations and improving patient care. However, these systems also present a significant cybersecurity risk, especially when vulnerabilities are discovered and exploited. One such vulnerability, CVE-2023-43208, highlights the critical need for robust security measures in healthcare organizations.

Understanding the Vulnerability

CVE-2023-43208 is an unauthenticated remote code execution vulnerability affecting NextGen Healthcare's Mirth Connect, an open-source data integration platform widely used in healthcare. This vulnerability stems from an incomplete patch for a previous command injection flaw (CVE-2023-37679). Successful exploitation allows attackers to execute arbitrary code on vulnerable systems, potentially gaining access to sensitive patient data, disrupting operations, and even compromising connected medical devices.

44%

of all Caresteam Vue systems in healthcare are vulnerable to CVE-2023-43208

25%

of PACs servers run an EOL OS

The Challenge

For CISOs in healthcare, this vulnerability presents a multifaceted challenge. Mirth Connect is a popular integration engine in healthcare, connecting various EHR systems, medical devices, and other healthcare applications. This widespread use increases the potential attack surface and the number of vulnerable systems. Legacy EHR systems and outdated integration platforms often accumulate technical debt, making them more susceptible to vulnerabilities like CVE-2023-43208.

Impact

The potential impact of a successful exploit is severe, including data breaches, ransomware attacks, disruption of critical healthcare services, and even patient safety risks. According to Armis Labs, 37% of healthcare delivery organizations have suffered more than two attacks. If we consider that outages as a result of cyberattacks can take weeks, often months, to return to normal operations, multiple consecutive attacks can leave an already vulnerable sector incapacitated.

While NextGen Healthcare has released a patch for this vulnerability, applying it across all affected systems can be complex and time-consuming, especially for large healthcare organizations with complex IT environments.

40%

of all healthcare organizations are vulnerable to CVE-2023-43208

17.8

On average, healthcare organizations have 17,8 assets exposed to CVE-2023-43208

Mitigation and Protection

The most effective way to mitigate the risks associated with CVE-2023-43208 is to apply the patched version 4.4.1 or later of Mirth Connect.

Isolating critical systems through network segmentation can limit an attacker's ability to move laterally within the network. By creating distinct segments for different parts of the organization, enterprises can contain the impact of a breach and protect sensitive data.

Even after patching or hardening, it is highly recommended to monitor impacted systems for anomalous behaviours. Use intrusion detection systems (IDS) or Web application firewalls (WAF) to monitor for suspicious activities. Regularly run vulnerability scans to identify and address potential misconfigurations or newer, unpatched vulnerabilities.

Conclusion

CVE-2023-43208 highlights the critical need for continuous vigilance and proactive security measures within healthcare organizations. This vulnerability, actively exploited by APT groups targeting the healthcare sector, underscores the importance of securing Electronic Health Records (EHR) systems and protecting sensitive patient data. CISOs should prioritize immediate remediation of CVE-2023-43208 to mitigate the risk of data breaches, operational disruptions, and potential compromises to connected medical devices. Failing to address this vulnerability exposes healthcare organizations to significant cybersecurity threats with potentially severe consequences for patient safety and data integrity.

Spotlight 2

Telehealth and Remote Monitoring Solutions

CVE-2024-39891

First Exploit Publish Date
July 23, 2024

CISA Due Date
August 13, 2024

The rapid adoption of telehealth and remote monitoring has transformed the way healthcare is delivered. This shift provides immense benefits for patients, healthcare providers, and overall efficiency in the medical field. However, with these advancements come substantial cybersecurity challenges. Overlooking the unique risks in telehealth and remote monitoring is crucial to protecting sensitive patient data and maintaining trust. The aforementioned APT groups are aware of this challenge and are actively exploiting it.

Understanding the Vulnerability

CVE-2024-39891 is an information disclosure vulnerability affecting the Twilio Authy API. It stems from an unauthenticated endpoint that processes requests containing phone numbers and responds with information about whether each number is registered with Authy. This flaw impacts Authy Android versions prior to 25.1.0 and Authy iOS versions prior to 26.1.0. Notably, this vulnerability was actively exploited in the wild as of June 2024, highlighting its significant risk to user privacy and data security.

9

The average Armis Risk Score for Telehealth Systems is 9 out of 10.

99.99%

Essentially all Telehealth Systems are based on an EOL Android OS

The Challenge

CVE-2024-39891 remains highly dangerous, particularly for organizations with exposed services or outdated patches. According to early Armis Labs assessments, this vulnerability is likely to still have exploitation attempts in the wild.

Mitigation and Protection

- Make sure to update to at least Authy Android v25.1.0 and Authy iOS v26.1.0.
- Ensure all devices receive regular firmware updates and enable automatic updates wherever possible.
- Maintain isolated networks for different systems, such as telehealth services and office administration. Network segmentation reduces the ability of hackers to move laterally within a system once they gain access.
- Even after patching or hardening, it is highly recommended to monitor impacted systems for anomalous behaviours. Use intrusion detection systems (IDS) or Web application firewalls (WAF) to monitor for suspicious activities. Regularly run vulnerability scans to identify and address potential misconfigurations or newer, unpatched vulnerabilities.

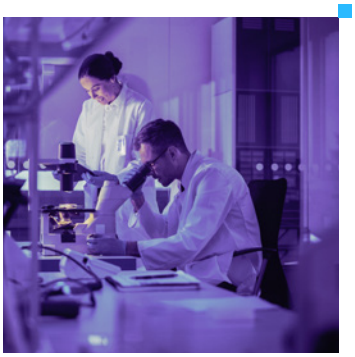
Conclusion

Telehealth adoption continues to increase and connected medical devices are predicted to surpass 29 billion by 2025 (Statista). Unfortunately, this growth also attracts cybercriminals, raising the stakes for securing these systems. By understanding CVE-2024-39891, assessing risks, and employing timely mitigation, you can significantly limit its potential impact on your organization.

Expanding the Focus: Additional Critical Systems

Armis Labs also recommends prioritizing security efforts to encompass the following systems, which are increasingly targeted by the same APT groups and other dominant threats detailed in this report:

Medical Imaging Systems including PACS (Picture Archiving and Communication Systems) by major vendors like GE Healthcare, Siemens, and Philips, play a crucial role in managing and storing medical images. Vulnerabilities within DICOM protocols, imaging data transfer mechanisms, and system integration points are targeted by malicious actors to disrupt operations, compromise data integrity, or gain unauthorized access to sensitive patient information.



Laboratory Information Systems (LIS) are essential for managing laboratory workflows and data, often relying on Windows Server and SQL Server platforms. Vulnerabilities in these underlying platforms or middleware components can expose LIS to cyberattacks, potentially leading to data breaches, disruption of laboratory operations, and delays in patient care.

Hospital Information Systems (HIS) serve as the backbone of healthcare organizations, integrating EHR, billing, and administrative functions. They often rely on Java-based or open-source platforms, making them susceptible to exploits like CVE-2021-44228 (Log4j) and similar middleware vulnerabilities. Exploiting these weaknesses can grant attackers extensive control over critical systems and sensitive data.

By expanding the focus to include these additional systems, healthcare organizations can further strengthen their security posture and mitigate the risk of cyberattacks that could compromise patient care, data integrity, and operational continuity.

High Impact Ransomware Groups

Healthcare Delivery Organizations (HDOs) are amongst the largest and most lucrative targets for ransomware attacks. Owing to the sensitive nature of the devices healthcare delivery organizations rely on, and the proximity to patient care of those devices, malicious actors have targeted HDOs for being more likely to pay ransomware demands to ensure continuity of patient care.

Armis Labs has unique visibility into the tactics of prevalent ransomware groups and provides crucial threat intelligence derived from analyzing billions of devices and extensive research.

Armis' asset- and threat intelligence indicate that multiple ransomware groups are actively targeting vulnerabilities commonly found within healthcare organizations. This necessitates immediate action to strengthen our security posture and mitigate the risk of a successful attack.

> **Specifically, we have observed increased activity related to exploitation of public-facing applications, RDP vulnerabilities, and phishing campaigns.**

This report provides an analysis of the Tactics, Techniques, and Procedures (TTPs) employed by prominent ransomware groups currently active. This information is vital for understanding the evolving threat landscape and enhancing our cybersecurity posture to protect patient data, critical systems, and ensure continued care delivery.

The overview below delves into the true impact of cyberwarfare in healthcare, and provides details about what Armis Labs considers to be the current most dominant Ransomware Groups. By understanding their attack patterns, we can proactively strengthen our defenses and mitigate the risk of falling victim to these threats.

LockBit 3.0	
Initial Access	Phishing, RDP exploitation, public-facing application vulnerabilities
Execution	Obfuscated payloads, boot autostart execution
Defense Evasion	File deletion, execution guardrails
Impact	Data encryption, service stoppage, and system recovery inhibition

ALPHV (BlackCat)	
Initial Access	Credential theft, Exchange vulnerabilities
Execution	Process injection, registry querying
Discovery	AdFind, ADRecon for Active Directory exploration
Impact	Inhibit system recovery, data encryption

BianLian	
Initial Access	Phishing emails, compromised credentials
Persistence	Account creation, registry modifications
Lateral Movement	RDP, credentials in files
Impact	Data encryption

Akira

Initial Access	Spear phishing, credential compromise
Execution	PowerShell, Windows command shell
Persistence	Domain account creation, scheduled task
Impact	Double extortion with encryption and data leaks

BlackSuit

Execution	User execution, process discovery
Discovery	File and directory reconnaissance
Impact	Data encryption, recovery inhibition

Hunters International

Initial Access	Modified Hive ransomware
Execution	Native API, shared modules
Impact	Focus on data exfiltration over encryption

Medusa

Initial Access	RDP vulnerabilities, phishing
Execution	PowerShell, shadow copy deletion
Impact	Data encryption with `.MEDUSA` extension

NoEscape	
Initial Access	Custom built ransomware, external remote services
Execution	Process termination, registry run keys
Impact	Multiextortion (encryption + data exfiltration)

INC RANSOM	
Initial Access	Spear phishing, exploitation of vulnerabilities
Execution	Native API, shared modules
Impact	Focus on data exfiltration over encryption

Meow	
Initial Access	Public facing application exploitation, phishing
Execution	ChaCha20 encryption
Impact	Data encryption with limited victim targeting

High Impact and Emerging Risks In Healthcare

Armis Labs leverages data from over 5 billion assets through the AI-driven Armis Asset Intelligence Engine, combined with deception technology, incident forensics, reverse engineering, dark web monitoring, and human intelligence. The data we gather helps to identify exploited and emerging CVEs, as well as the dominance and impact of those attacks. During Q4, 2024 we have identified the following CVEs widely exploited in healthcare environments, through diverse medical devices and IT systems:

CVE	Title	Criticality	First Intel Hit	First Hit Date	% Estimated organizations vulnerable to this CVE
CVE-2021-44228	Remote code execution in Log4j library	Critical - widespread exploitation	Oct 18th, 2021	Dec 10, 2021	**40%**
CVE-2020-0601	Windows CryptoAPI digital certificate spoofing	High - allows malware to appear trusted	Jan 14th, 2020	Jan 14th, 2020	**60%**
CVE-2023-42793	Windows Kernel elevation of privilege (local access)	High - potential for complete system takeover	Sept 30th, 2023	Sept 30th, 2023	**N/A**
CVE-2023-23397	Microsoft Outlook elevation of privilege via malicious email	High - unauthorized access to Outlook data	March 15th, 2023	March 15th, 2023	**80%**

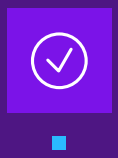
While not actively exploited yet in healthcare environments, these CVEs are drawing attention from threat actors:

CVE	Title	% Estimated organizations vulnerable to this CVE
CVE-2016-6272	The MyChart software contains an X-Path injection due to the lack of sanitization for the GE parameter “topic”. A remote attacker can access contents of an XML document containing static display strings, such as field labels, via the topic parameter to help.asp.	Emerging Threat
CVE-2021-36385	A SQL Injection vulnerability in Cerner Mobile Care 5.0.0 allows remote unauthenticated attackers to execute arbitrary SQL commands via a Fullwidth Apostrophe (aka U+FF07) in the default.aspx User ID field. Arbitrary system commands can be executed through the use of xp_cmdshell.	Emerging Threat
CVE-2015-2899	Heap-based buffer overflow in the QualifierList retrieve_qualifier_list function in Medicomp MEDCIN Engine before 2.22.20153.226 might allow remote attackers to execute arbitrary code via a long list name in a packet on port 8190.	Emerging Threat
CVE-2023-50164	An attacker can manipulate file upload params to enable paths traversal and under some circumstances this can lead to uploading a malicious file which can be used to perform Remote Code Execution. Users are recommended to upgrade to versions Struts 2.5.33 or Struts 6.3.0.2 or greater to fix this issue.	13%
CVE-2023-22071	Vulnerability in the PL/SQL component of Oracle Database Server. Supported versions that are affected are 19.3-19.20 and 21.3-21.11. Easily exploitable vulnerability allows high privileged attackers having Create Session, Execute on sys.utl_http privilege with network access via Oracle Net to compromise PL/SQL. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PL/SQL, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PL/SQL accessible data as well as unauthorized read access to a subset of PL/SQL accessible data and unauthorized ability to cause a partial denial of service.	13%
CVE-2012-6693	GE Healthcare Centricity PACS 4.0 Server has a default password of (1) nasro for the nasro (ReadOnly) user and (2) nasrw for the nasrw (Read/Write) user, which has unspecified impact and attack vectors.	20%
CVE-2018-17906	Philips iSite and IntelliSpace PACS, iSite PACS, all versions, and IntelliSpace PACS, all versions. Default credentials and no authentication within third party software may allow an attacker to compromise a component of the system.	Emerging Threat
CVE-2013-7442	GE Healthcare Centricity PACS Workstation 4.0 and 4.0.1 has a password of (1) CANal1 for the Administrator user and (2) iis for the IIS user, which has unspecified impact and attack vectors related to TimbuktuPro. NOTE: it is not clear whether this password is default, hardcoded, or dependent on another system or product that requires it.	20%

Conclusion and Best Practices

Healthcare organizations must take a holistic approach to cybersecurity, from conducting regular asset inventories and vulnerability assessments to ensuring that security policies are regularly updated to reflect the current attack landscape. It's crucial to factor in the clinical context of every asset when prioritizing cybersecurity efforts, as well as investing in regular penetration testing and continuously assessing risk in the ever-changing healthcare environment.

Cybersecurity Health Checks



Comprehensive Asset Inventory Management: Leverage advanced asset intelligence platforms like Armis Centrix™ to maintain a real-time, dynamic inventory of all healthcare devices—from medical IoT and legacy systems to network infrastructure—ensuring every asset is continuously monitored, properly categorized, and integrated into security workflows.

Contextualized Vulnerability Prioritization: Factor in the clinical importance and patient safety implications of each asset when prioritizing remediation efforts. For example, a vulnerability in a critical diagnostic imaging system should receive a higher priority than one in a non-critical administrative device.

Early Warning Vulnerability Alerts: Adopt “early warning” intelligence feeds that highlight newly weaponized and actively exploited vulnerabilities. Use this intelligence to respond swiftly and proactively, patching critical issues before attackers widely leverage them.

Continuous Risk Scoring and Assessment: Move from point-in-time assessments to continuous risk evaluation. Automatically update risk scores as new threats emerge, vulnerabilities are discovered, or devices come online, ensuring that security posture adapts to the evolving threat landscape.

Regular Security Policy Audits and Updates: Periodically review and update security policies to reflect the latest threat trends and compliance requirements. Integrate new insights from threat intelligence sources and recent vulnerability disclosures into policies and controls.

Clinical-Informed Security Controls: Collaborate with clinical engineering, biomedical technicians, and frontline caregivers to understand the real-world usage of medical devices. Implement tailored controls that protect these systems without disrupting patient care or clinical workflows.

Cybersecurity Health Checks

Rigorous Penetration Testing and Simulated Attacks: Conduct regular penetration tests by internal security teams or trusted third parties. Simulate real-world attack scenarios to identify weak points and validate incident response plans, ensuring the organization can withstand increasingly sophisticated threats.

Network Segmentation and Micro-Segmentation: Segment critical medical networks from less sensitive areas to limit lateral movement by attackers. Implement micro-segmentation to create granular security zones around critical assets, reducing the blast radius of successful intrusions.

Incident Response Readiness and Drills: Develop and maintain a well-defined incident response plan. Conduct tabletop exercises and simulated breaches to train staff, refine response protocols, and ensure readiness to act swiftly when an actual incident occurs.

Ongoing Security Training and Awareness: Provide regular cybersecurity training and education for all staff—clinicians, IT personnel, and administrators alike. Emphasize how their actions influence security, from recognizing phishing attempts to following best practices for handling patient data.

The path to better cybersecurity in healthcare is not an easy or straightforward one. It involves a constant cycle of monitoring, updating, testing, and adjusting based on new threats and vulnerabilities. However, it is a path worth treading because it ensures the secure delivery of critical care to patients and protects healthcare organizations from the devastating financial and operational impact of (ransomware) attacks. Our advice to healthcare organizations is clear: Invest in threat detection and early warning systems, embed cybersecurity into the fabric of your culture and operations, and take a preventive, proactive approach to safeguard your organization and your patients against cyber threats.

ARMIS LABS

About Armis Labs

Armis Labs, a division of Armis, is a team of seasoned security professionals dedicated to staying ahead of the ever-evolving cybersecurity landscape. With a deep understanding of emerging threats and cutting-edge methodologies, Armis Labs empowers organizations with unparalleled visibility and expertise to protect against the threats that matter most, right now.

At the heart of Armis Labs lies a formidable research powerhouse, where experts investigate the latest trends and tactics employed by cyber adversaries. Armed with access to over 5 billion profiled assets and state-of-the-art tools and methodologies, the team at Armis Labs conducts in-depth analyses of evolving threats both in the pre-emergence stage and “in the wild” stage of an attack.

+5 Billion

Core to Armis Labs is our Asset Intelligence Engine. It is a giant, crowdsourced, cloud-based knowledge base - the largest in the world, tracking over five billion assets - and growing. It powers Armis Labs with unique, actionable cyber intelligence to detect and address real-time threats across the entire attack surface.

Armis Labs security practitioners are utilizing cutting edge technology that include dynamic honeypots, incident forensics, reverse engineering, dark web monitoring, and human intelligence to proactively identify and mitigate threats before they manifest. Leveraging advanced AI/ML technologies, Armis Labs’ proactive threat detection capabilities enable organizations to stay one step ahead of cyber adversaries, minimizing the risk of potential breaches while stopping potential damage before it occurs.

Armis Labs is dedicated to providing organizations with the tools and expertise they need to defend against the threats that matter most, right now. With comprehensive threat intelligence, proactive threat detection capabilities, and seamless integration into existing security workflows, Armis Labs empowers organizations to stay ahead of cyber adversaries and protect their most critical assets.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial