2023 State of Cybersecurity for Medical Devices and Healthcare Systems

FINITE STATE

Securin

Health-ISAC™

Table of Contents

Foreword

By Phil Englert, VP for Medical Device Security, Health-ISAC

Improving patient safety and protecting healthcare from cybersecurity threats is our top priority at Health-ISAC. The healthcare sector is essential to a country's national security infrastructure. Cyber-attacks on healthcare systems can have broader implications for public health and national security.

If hackers gain unauthorized access to medical records or alter patient data, it can result in misdiagnosis, incorrect treatment plans, or delayed care. In severe cases, patients' lives could be at risk. Protecting medical histories, test results, insurance details, and personal information is crucial to maintain patient privacy and confidentiality. Breaches can lead to identity theft, fraud, or exposure to highly sensitive medical conditions. Cyber espionage or intellectual property theft can undermine medical research, stalling medical advancements. Modern healthcare relies heavily on interconnected systems and medical devices. If these systems lack adequate cyber security, they become entry points for intruders who can infiltrate the broader healthcare network.

While the health sector has made much progress in improving cyber resilience over the last decade, the research and analysis in this report continue to shed light on the depth and breadth of challenges that exist to secure the healthcare ecosystem. Health-ISAC continues to build a global healthcare community to empower trusted relationships to prevent, detect, and respond to cybersecurity and physical security events so that organizations can focus on improving health and saving lives. Health-ISAC continues to team with leading security firms to provide valuable resources for our members to identify and secure their environments.

Report Overview

The 2023 State of Cybersecurity for Medical Devices and Healthcare Systems report finds that the software and firmware powering connected medical devices and healthcare applications are increasingly at risk due to numerous critical and high-rated vulnerabilities.[1]

The research, conducted collaboratively by Securin, Finite State, and Health Information Sharing and Analysis Center (Health-ISAC), focused on analyzing credible public disclosures of cyber vulnerabilities. This analysis specifically targeted medical devices, software applications, and healthcare systems. The research assessed a total of 117 medical device and healthcare application vendors along with their 966 products.

[1]A vulnerability is a weakness or flaw or fault in the system which can be exposed to an attacker.

HIPAA VIOLATION PENALTIES

Since 2003, the OCR has investigated and resolved over 320,000 HIPAA complaints and settled or imposed civil money penalties totaling more than $135 million.

INTRODUCTION

Healthcare, as a sector, is classified by the US Government as one of the 16 critical infrastructures. It has increasingly become a prime target for cyberattacks, with potential consequences ranging from network disruptions to compromised medical equipment that could lead to fatal outcomes.

With 300 data breaches reported in the first half of 2023 alone, the healthcare sector is facing an unprecedented challenge in safeguarding sensitive information from malicious actors. Attackers have long found it profitable to hold healthcare centers and hospitals for ransom by stealing patient data. As reported by IBM, the average cost of a data breach in 2023 was estimated to be a staggering $11 million.

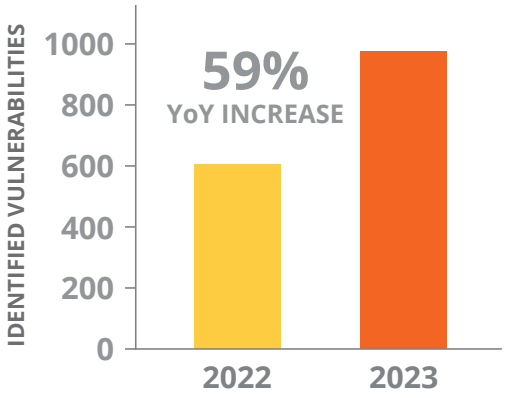
Furthermore, compliance is a key driver for healthcare organizations with regulations like the Health Insurance Portability and Accountability Act (HIPAA) and the need to protect patient data. A number of cyberattacks have had direct or indirect impact such as leaked personal information, disruption of care, and patient fatalities. An example of leaked personal information can be seen from the attack on a health system attributed to Cl0p ransomware, which compromised the personally identifiable information (PII) of 1 million customers. Another consequence caused by cyberattacks is disruption of care for patients as noted by the American Medical Association after documenting the effects of ransomware on healthcare providers. Tragically, the consequences of these cyberattacks on healthcare institutions can be severe. After a ransomware attack on a medical center, an infant died when neonatal staff were cut off from fetal heartbeat monitors caused by a network outage in the wake of the attack.

In this highly vulnerable industry, the impacts of cyberattacks extend far beyond financial losses and legal ramifications, and pose a significant threat to both patient care and safety, as well as the integrity of healthcare organizations. These incidents have demonstrated the critical vulnerabilities within the healthcare sector, underscoring the urgent need for a comprehensive understanding of the current threats and their far-reaching consequences.

In the following research findings, we aim to delve deeper into the evolving nature of cyber threats faced by healthcare organizations and to shed light onto the types of impacts on healthcare. We aim to emphasize the necessity of robust cybersecurity measures to safeguard sensitive medical data and ensure the continuity of essential healthcare services.

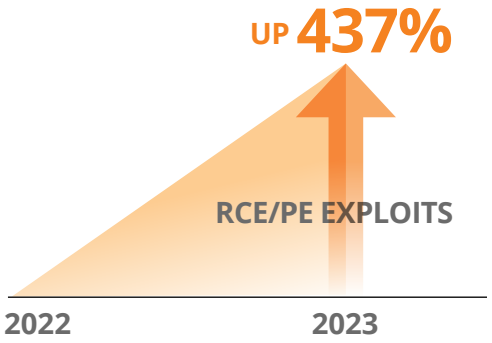
KEY RESEARCH FINDINGS

1. **993 vulnerabilities were found in 2023** (a 59% increase from 2022) spanning 966 healthcare products; these vulnerabilities can potentially be exploited by attackers to target healthcare organizations



2. **160 vulnerabilities are weaponized**, meaning they have a working Proof of Concept (PoC) that demonstrates how an attacker could exploit them, and 101 are trending in the wild, vulnerabilities that are currently spreading to real-world devices used by everyday users

3. **43 vulnerabilities are categorized as Remote Control Execution/Privilege Escalation (RCE/PE) exploits**, up 437% since 2022; these vulnerabilities are highly appealing to hackers as they enable remote access to networks, granting administrative control, and compromising systems

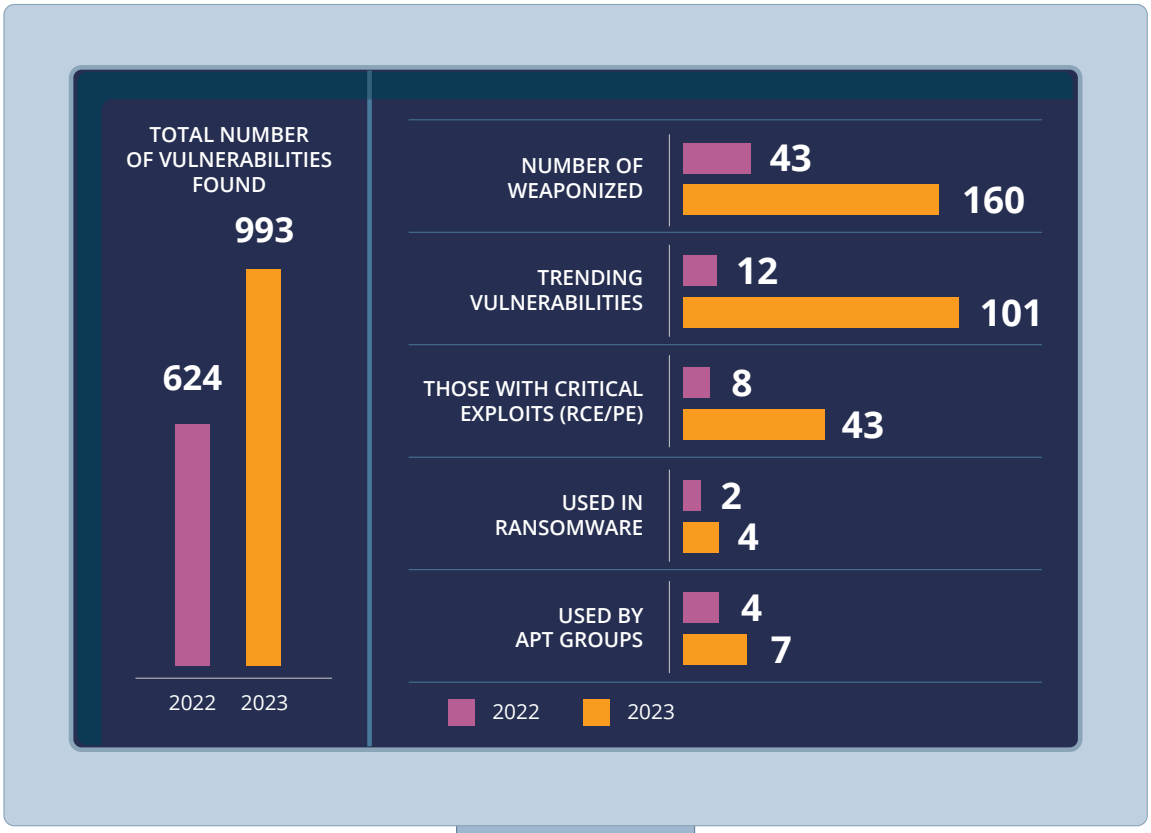


4. **7 vulnerabilities are exploited by Advanced Persistent Threat (APT) Groups**, threat actors who stay hidden within a system to steal data, and 4 vulnerabilities are associated with ransomware, a malicious virus that locks a user out of their system or encrypts data and demands a ransom for user retrieval

5.

CLASS I MEDICAL DEVICES	CLASS I I MEDICAL DEVICES	CLASS III MEDICAL DEVICES	HEALTHCARE IT
25 VULNERABILITIES	292 VULNERABILITIES	2 VULNERABILITIES	741 VULNERABILITIES

COMPARISON OF VULNERABILITIES 2022-23



HIPAA VIOLATION PENALTIES

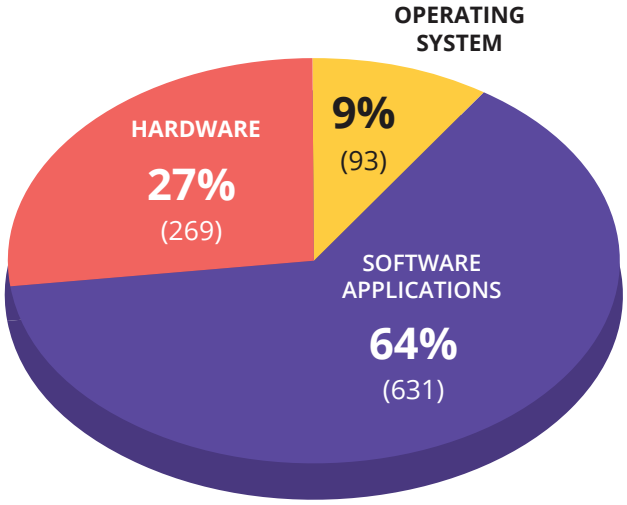
In 2020, the OCR settled multiple HIPAA cases, resulting in penalties ranging from $10,000 to $6.85 million, with settlements totaling over $13.5 million.

Vulnerabilities Across Product Types

The research was conducted across 117 medical device and healthcare application vendors that constituted over 966 products. In those products, 993 vulnerabilities were found across medical hardware, operating systems, and software applications.

Software applications used in the healthcare sector account for the highest percentage (64%) of vulnerabilities found. Healthcare applications are crucial for managing patient care, appointment scheduling, and accessing medical records. Many medical devices (such as infusion pumps, pacemakers, and monitoring systems) also rely on software applications. Therefore, vulnerabilities in these applications can enable attackers to disrupt essential healthcare services, leading to delayed treatments or compromising the functionality of medical devices, potentially endangering patients' lives.

VULNERABILITIES BY PRODUCT TYPE



Hardware vulnerabilities were the next largest group with 27% of vulnerabilities. Tools such as hardware are indispensable in the healthcare sector. These aid in patient care, diagnosis, treatment, and monitoring. From everyday computers to life-support systems, hardware improves medical capabilities and patient outcomes. However, vulnerabilities in healthcare hardware can pose serious risks, including compromised patient care, operational disruptions, and loss of trust.

There are not as many Operating System vulnerabilities with only 9%, but they are still present. These vulnerabilities leave an open door to manipulation of medical devices, unauthorized access to healthcare systems, and non-compliance with data protection regulations.

HEALTHCARE DEVICE CLASSIFICATIONS AND SYSTEMS

Healthcare devices are classified into different categories based on their intended use, potential risks, and level of regulation.

Class I *(e.g. bandages, transportation, and monitoring stations)*

These are low-risk devices that are simple in design and have minimal potential to cause harm to the user. Class I devices are subject to the least regulatory control.

Class II *(e.g. anesthesia monitoring, infusion pumps, and CT scanners)*

These devices are considered moderate risk and require more stringent regulation than Class I devices. They often have special controls in place to ensure their safety and effectiveness.

Class III *(e.g. pacemakers, heart valves, and certain types of implantable devices)*

These are high-risk devices that are intended to sustain or support life, or are implants that are critical to the body's functioning. These devices undergo the most rigorous regulatory scrutiny to ensure their safety and effectiveness.

Healthcare IT *(software, applications, IT infrastructure in support of healthcare operations)*

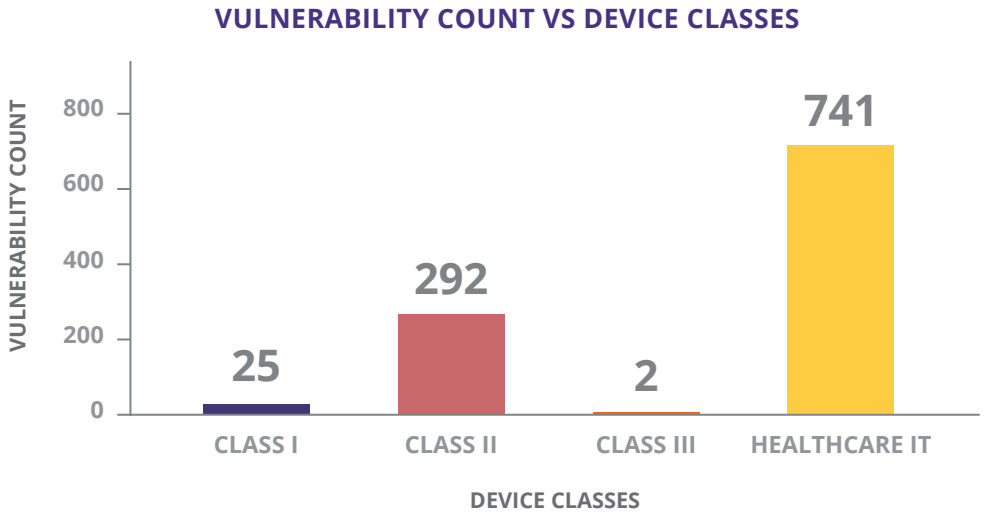
Healthcare IT involves the use of technology and information systems to manage and store medical data and patient information. It has several important aspects, one of which is the handling of highly sensitive medical data and personally identifiable information (PII).

HIPAA VIOLATION PENALTIES

The largest HIPAA settlement to date was in 2019 when OCR fined a healthcare provider $16 million for multiple violations.

Category	Product Types	Products (Count)	Vulnerabilities (Count)	Classes of Medical Devices
CRT-D\Implantable Cardioverter Defibrillators (ICDs)	Cardiac Resynchronization Therapy Defibrillators, Implantable Cardioverter Defibrillators (ICDs), Pacemakers	20	2	Class – III
Continuous Renal Replacement Therapy	Dialysis, Fluid Management, Ultrafiltration	3	4	Class – II
Surgical Theater	C-ARMs, Vessel Sealing systems, Surgical Navigation systems etc.	13	8	Class – II
Medical Infusion Pump	IV, Syringe, Insulin, PCA (Patient-Controlled Analgesia) Pumps etc.	67	58	Class – II
Anesthesia Station	Anesthesia Monitoring & Dispensing Stations	4	4	Class – II
Medical Monitoring/ Telemetry	ECG/EKG, Cardiac, Blood-Pressure, Gluco Monitors etc.	89	129	Class – II
Medical Imaging	Ultrasound, MRIs, CT Scanners, X-Rays, Digital Radiography devices	185	84	Class – II
Clinical Analyzer	Cyclotrons, Blood Gas Analyzers, Hematology Analyzers etc.	6	5	Class – II
Medical Inventory/ Dispensing Systems	RFID-Based Inventory Systems, Pharmaceuticals Inventory Management, Automated Medication Dispensing Carts etc.	20	12	Class – I
Medical Robotics	Delivery & Transportation, Mobility Robots	21	13	Class – I
Healthcare IT	Health Applications, EHRs, Database Management & Servers	538	741	Healthcare IT App

Class I devices, though more basic compared to the other classes, play a crucial role in daily patient care. This class exhibited some vulnerabilities, with 25 identified across 41 products, potentially impacting medical transportation, pharmaceuticals inventory, and automated medication dispensing carts. Moving on to Class II devices, they face more regulation due to their moderate-risk classification. Within this category is a high number of vulnerabilities with 292 discovered across 367 products, including anesthesia stations, CT scanners, and medical infusion pumps. Even Class III devices, which are essential for sustaining and supporting life, were found to have 2 vulnerabilities across 20 products, making them susceptible to potential attacks. This emphasizes the urgent need for robust cybersecurity measures in the healthcare industry to safeguard devices crucial to patients' well-being.



Healthcare IT faces significant risks concerning the handling of highly sensitive medical data and personally identifiable information (PII) and it is shown how vulnerable they are with a count of 741 vulnerabilities across 538 products. Patient privacy concerns arise due to the vast amount of confidential information stored in healthcare systems, making them susceptible to security breaches and potential exposure of patient data. Compliance with data protection regulations, data encryption, and strict access controls are vital to mitigate these risks.

Vulnerabilities Associated With Threat Actors

ADVANCED PERSISTENT THREAT (APT) GROUP ASSOCIATIONS

Advanced Persistent Threat (APT) groups are highly skilled and organized cyber threat actors that conduct advanced and targeted attacks, often with state support, to steal sensitive data or disrupt critical infrastructure. APT groups continue to strike at the healthcare sector as The U.S. Department of Health and Human Services' (HHS) Health Sector Cybersecurity Coordination Center (HC3) warns of four Russian state-backed groups that pose significant threats, including Turla, APT29, APT28, and Sandworm.

Vulnerabilities	Technical Impact	APT Association
CVE-2021-45105	Denial of Service[2]	APT 27 — EmissaryPanda
CVE-2020-11022 **CVE-2019-11358** **CVE-2015-9251** **CVE-2021-45105**	Remote Code Execution[3] Denial of Service Information Disclosure/Remote Code Execution Denial of Service	APT 1 — BrownFox APT 27 — EmissaryPanda
CVE-2020-11023 **CVE-2019-11358** **CVE-2015-9251** **CVE-2021-45105**	Remote Code Execution Denial of Service Information Disclosure[4]/Remote Code Execution Denial of Service	APT 1 — BrownFox APT 27 — EmissaryPanda
CVE-2020-11023, **CVE-2021-45105**	Remote Code Execution Denial of Service	APT 1 — BrownFox APT 27 — EmissaryPanda
CVE-2021-45105	Denial of Service	APT 27 — EmissaryPanda
CVE-2021-44832	Remote Code Execution	APT 34 — Helix Kitten, APT 35 — Charming Kitten APT 42 — Crooked Charms
CVE-2021-34527	Remote Code Execution	APT 41 — Earth Longzhi

[2]A type of cyberattack aimed at disrupting the normal functioning of a system or online service through overwhelming the target with an excessive amount of traffic, requests, or data.

[3]An attacker can take control of a device or system without needing physical access to it.

[4]Sensitive data is unintentionally or maliciously exposed to unauthorized individuals.

State-sponsored actors are persistently going after key infrastructure and the Healthcare industry has been no exception. Research indicates that some vulnerabilities previously exploited by APT groups are still present within vendor products and pose a greater risk given they have been proven already.

Four of the vulnerabilities are associated with APT1 or the BrownFox group, a Chinese-sponsored actor in existence since 2006. The remaining three vulnerabilities are exploited by numerous APT groups.

This is particularly concerning, as medical device vendors could face regulatory investigations from the FDA, civil lawsuits, and product liability claims for non-compliance with cybersecurity standards and endangering device safety.

RANSOMWARE ASSOCIATIONS

The FBI released a report on cyberattacks highlighting healthcare as one of the top sectors to experience ransomware attacks among all critical infrastructure sectors in 2022. These malicious incidents, characterized by the encryption and hostage of sensitive data, have become an ever-present concern for healthcare providers.

One concerning aspect of these attacks is the targeting of surgical navigation technologies that are widely utilized by surgeons in operating rooms today. These sophisticated technologies play a crucial role in guiding surgeons during complex procedures, providing real-time information and precise navigation within the patient's body. The dangerous PrintNightmare vulnerability affecting the technology is actively exploited by three ransomware groups, including the highly active Conti ransomware. The consequences of such attacks can be devastating, as they have the potential to impede ongoing surgeries or prevent critical procedures from taking place.

The threat of ransomware attacks is increasing exponentially among healthcare providers since the pandemic. As healthcare organizations continue to embrace digital transformation and rely heavily on interconnected systems, the potential for devastating data breaches looms larger than ever before.

Product Type	Vulnerability	Ransomware Association
Operating System	CVE-2020-0601	BigBossHorse
Application	CVE-2021-34527	Cerber, Conti, Vice Society

Conclusion and Recommendations

The danger of cyber attacks targeting healthcare is very real. Considering the possibility of devastating consequences if such attacks are successful, it's crucial for organizations to take proactive measures towards addressing the vulnerabilities in the medical devices and applications utilized in the healthcare industry.

To protect against cyber attacks, there are several steps that healthcare organizations must adopt the following:

1. **Implement a regular penetration testing cadence or exposure assessment:** This helps identify possible exposures in the attack surface, allowing organizations to address vulnerabilities before they can be exploited.

2. **Prioritize vulnerability patching based on known risks:** By staying updated with the latest security vulnerabilities and promptly applying relevant patches, organizations can significantly reduce the risk of successful cyber attacks.

3. **Evaluate binary analysis tools:** Incorporating binary analysis tools as part of the overall security strategy enables organizations to generate Software Bill of Materials (SBOM) and leverage the results for penetration testing. This helps uncover potential vulnerabilities and aids in securing the healthcare ecosystem.

4. **Mandate vendors to follow "security by design" methodology:** With the FDA's latest guidance emphasizing "security by design," it is essential for healthcare organizations to require their vendors to adopt this methodology. By incorporating security practices throughout the entire development lifecycle, from design to deployment, vendors can build more resilient and secure medical devices and applications.

Research and Technology

Securin's Research and Methodology:

- Securin's platform powered by its Vulnerability Intelligence (VI) enabled the team to conduct this research.
- Of the 993 vulnerabilities analyzed, 6 have already been used in critical cyberattacks and pose a significant threat to healthcare organizations. However, long before these attacks could take place, Securin had flagged 5 of these CVEs and predicted their exploitability.
  - CVE-2020-2555 was first identified on February 9, 2020 and continues to be trending in 2023. An exploit was published 152 days after Securin flagged it for its high probability of exploitation.
  - CVE-2020-1938 was detected by Securin as a Zero Day across the dark web 49 days before the vendor assigned a CVE ID to the vulnerability.
  - CVE-2017-17562 was published by the US Cybersecurity and Infrastructure Security Agency (CISA) in its Known Exploited Vulnerability (KEV) catalog 4 years after its exploit was published.
  - CVE-2021-34527 is part of the arsenal of DEV-0832 or Earth Longzhi, a dangerous threat actor, and is associated with ransomware such as Magniber, Vice Society, Ransom Cartel, Conti, and Black Basta.
  - CVE-2020-0601 is associated with the Horsedeal ransomware and was added to the CISA KEVs 483 days after the exploit was published.

Finite State Methodology:

- The creation of Software Bill of Materials (SBOMs) for firmware, combined with the identification of Common Vulnerabilities and Exposures (CVEs) through binary analysis, significantly surpasses security analysis solely based on CVEs. This holistic approach offers a more comprehensive view of system vulnerabilities by considering not only documented flaws but also latent vulnerabilitiesresiding in the binary code.

- An Internet of Things (IoT) device was initially identified as having 3 CVEs, which rendered it susceptible to specific threats. However, the application of binary analysis and subsequent SBOM generation revealed a staggering 993 CVEs associated with the same device. The nearly 300-fold increase in identified vulnerabilities dramatically underscores the importance of this integrated approach, providing a far more accurate and thorough risk assessment and enhancing the effectiveness of subsequent mitigation strategies.

- 6,000 critical and high vulnerabilities were found in one updated firmware product, showing an 18x increase over the previous version.

Glossary

Attack Surface — The sum of both known and unknown assets in an organization that are visible to the internet (i.e., desktop computer, email server, third-party vendors).

Advanced Persistent Threat (APT) — Threat actors with a sophisticated level of expertise who stay hidden within a system or network to steal data.

Common Vulnerability and Exposures (CVE) — A CVE is an ID assigned to a vulnerability by the CVE Numbering Authority (CNA). After being analyzed the vulnerability is publicly listed in MITRE and updated to the National Vulnerability Database (NVD).

Denial of Service (DoS) — A type of cyberattack aimed at disrupting the normal functioning of a computer system, network, or online service through overwhelming the target with an excessive amount of traffic, requests, or data.

Exploit — Code designed to take advantage of security flaws or vulnerabilities to help attackers gain high-level access to a network, move laterally, and compromise an organization's entire IT infrastructure.

Information Disclosure — An incident where sensitive or confidential data is unintentionally or maliciously exposed to unauthorized individuals.

Privilege Escalation — Privilege escalation is used by attackers to gain higher access to a system or network by taking advantage of a weakness.

Ransomware — Ransomware is a malicious virus that locks a user out of their system or encrypts data and demands a ransom for user retrieval of their system or data.

Remote Code Execution (RCE) — RCE is a type of vulnerability where an attacker can take control of a device or system without needing physical access to it.

Trending in the Wild — Trending in the Wild refers to vulnerabilities that are currently spreading to real world devices used by everyday users.

Vulnerability — Vulnerability is a weakness or flaw or fault in the system which can be exposed to an attacker.

- **Low –** Low-level vulnerabilities, typically require physical access and have little to no impact on the business or its security and have the longest open window to be resolved.
- **Medium –** Medium vulnerabilities require additional measures like social engineering to be exploitable and offer only limited access; should be resolved within 1–3 months.
- **High –** High vulnerabilities are a higher level of difficulty but remain exploitable, potentially leading to escalated privileges, data loss, or downtime. Resolving such vulnerabilities should be prioritized within 4 weeks to 3 months.
- **Critical –** Critical vulnerabilities are highly compromisable leading to root-level exposure. These patches demand immediate remediation upon discovery within 2 weeks to 2 months.

Weaponized — A vulnerability with a working Proof of Concept (PoC) that demonstrates how an attacker could exploit it.

About Finite State

Finite State empowers organizations to gain control of application and product security for their connected devices and software supply chains. Across the software supply chain lifecycle, Finite State is the single pane of glass for customers that provides continuous visibility into software supply chain risk.

Backed by a team of seasoned experts, Finite State's platform arms customers with the automation to scale risk mitigation and 2B+ data points to deliver actionable SBOM's and insights, critical vulnerability data and the remediation guidance necessary to mitigate AppSec and product risk to protect the connected attack surface.

About Health-ISAC

Health-ISAC — a non-profit, private sector, member-driven organization — plays an essential role in providing situational awareness around cyber and physical security threats to the Healthcare Sector so that companies can detect, mitigate, and respond to ensure operational resilience. Health-ISAC connects thousands of healthcare security professionals worldwide to share peer insights, real-time alerts, and best practices in a trusted, collaborative environment. As the go-to source for timely, actionable, and relevant information, Health-ISAC is a force-multiplier that enables healthcare organizations of all sizes to enhance situation awareness, develop effective mitigation strategies and proactively defend against threats every single day.

About Securin

Securin is a leading provider of tech-enabled cybersecurity services, helping customers gain resilience against emerging threats. Our products and services are powered by accurate vulnerability intelligence, human expertise, and automation, enabling enterprises to make critical security decisions to manage their expanding attack surfaces.

FINITE STATE | Securin | Health-ISAC™ Collaborating for Resilience in Healthcare