



MARCH 2025 UPDATE

WHAT THE MEDICAL DEVICE INDUSTRY CAN LEARN FROM PAST CYBERSECURITY VULNERABILITY DISCLOSURES

Since the FDA released their Postmarket Cybersecurity Guidance in 2016, the monthly rate of ICS-CERT medical device advisories has increased by 386%, but appears to have plateaued from 2022 through 2024.

*This is an updated version based on an analysis of 2013 through 2024 ICS-CERT advisories analyzing trends in cybersecurity vulnerability disclosures.

EXECUTIVE SUMMARY

Reflecting on 2024, medical advisories from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) indicate that medical device vulnerabilities continue to be a significant concern. 2025 furthered this with a first quarter FDA/CISA [patient safety alert](#) where a vulnerability could, if exploited, allow for remote code execution, unauthorized upload of files, and compromise of confidential patient data.

Vulnerabilities underscore the persistent challenges in medical device cybersecurity, even years after the FDA's 2016 postmarket cybersecurity guidance. The vulnerabilities reported in 2024 highlight areas where manufacturers may not have fully implemented the FDA's recommendations, particularly in:



Access Control

The presence of hardcoded credentials and the absence of login attempt limits suggest insufficient access control measures.



Data Integrity

The ability to manipulate medical images indicates a lack of robust data validation and integrity check



Software Update Mechanisms

Inadequate integrity checks during firmware updates point to weaknesses in the software postmarket maintenance process.

The FDA's 2016 guidance emphasized the need for manufacturers to proactively manage cybersecurity risks, including routine updates and patches, and to establish a coordinated vulnerability disclosure policy. The recurring nature of these vulnerabilities suggests that continuous improvement in these areas is essential.

Why we wrote this report

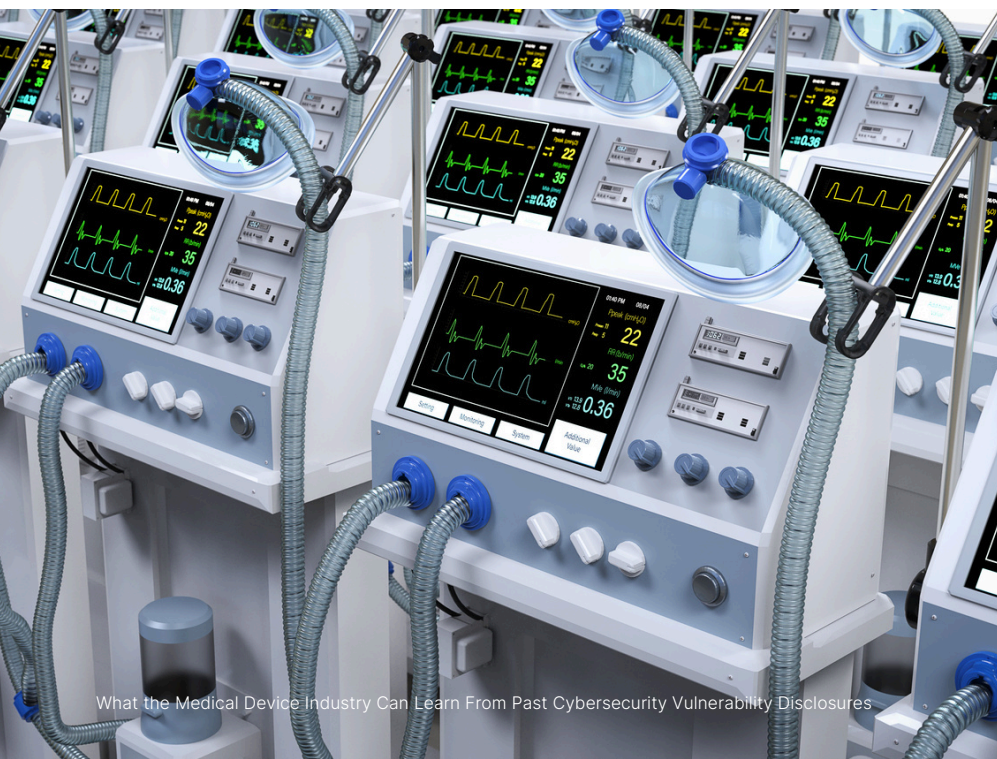
Many security vendors have an element of fear, uncertainty, and doubt as part of a sales tactic. That isn't how we operate. So in an effort to find data to substantiate our view of the space, we turned to vulnerability disclosures. We think data-driven insights provide actionable learnings for all device manufacturers, regardless of size/clinical focus or otherwise. And by sharing the data openly, we hope to collaborate with others interested in making evidence-based security decisions.

What we recommend

Vulnerability management can be difficult and time-consuming, but there are opportunities for improvement, better business value, and ROI at every stage of maturity. The dozens of low level, pervasive vulnerabilities that have impacted medical devices in recent years (think: rsync) demonstrate that all companies need to be prepared. There are enough incentives ([including President Biden's executive order](#) and FDA's increased scrutiny on vulnerability management), that the time to mature your programs is now.

A note on the inclusion of vendor names

We consider the inclusion of a specific medical device manufacturer's (MDM) name in the list of companies below to be a positive indicator of their active management of cybersecurity risk. All technology carries cybersecurity risk, therefore the sharing of medical device cybersecurity advisories is a positive and expected outcome of MDM's postmarket cybersecurity management. Medical device manufacturers who actively disclose and address cybersecurity vulnerabilities should be applauded for embracing and applying resources to the disclosure and sharing process.



SECTION I: DATA

We reviewed the [ICS-CERT Advisory Database](#), which includes vulnerability disclosures originating from manufacturers, researchers, or were the result of a coordinated vulnerability disclosure, to identify all advisories related to medical devices.

For detailed data description, see Appendix A, as well as raw data [here](#).

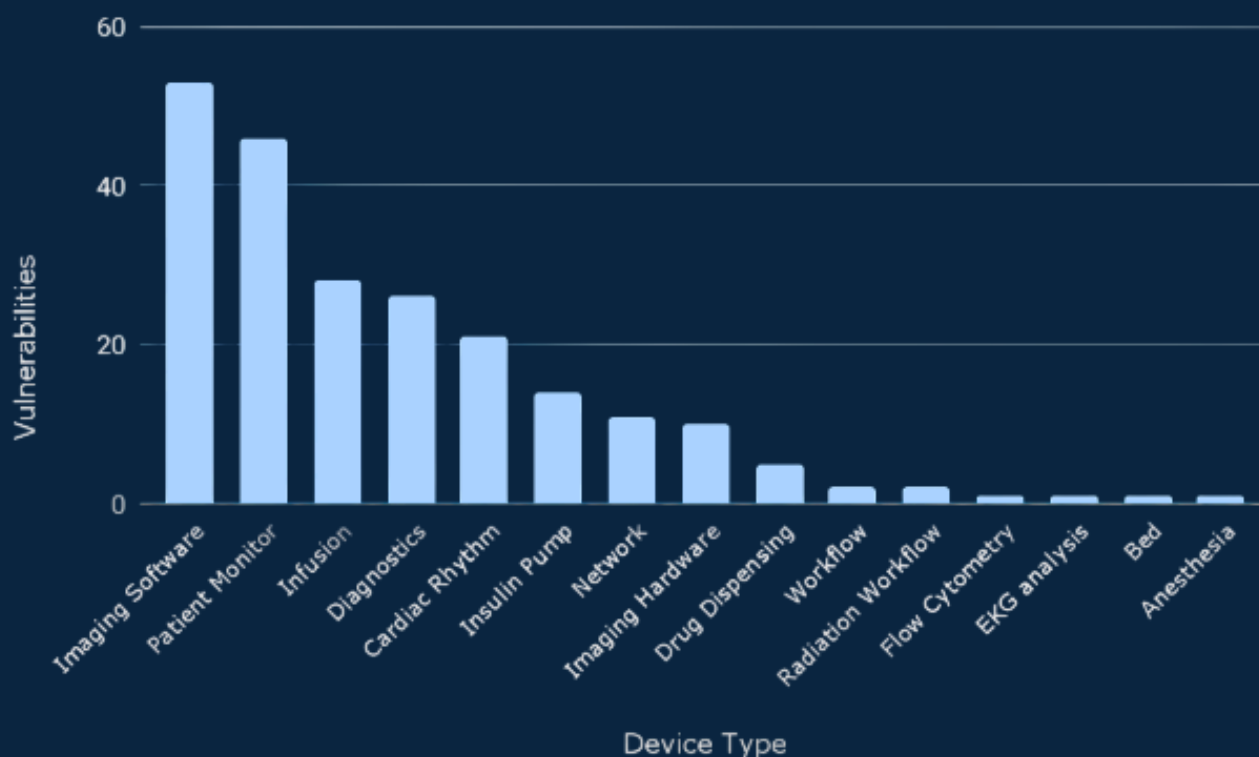
SECTION II: OBSERVATIONS FROM THE DATA

Root Causes Haven't Changed

Vulnerabilities attributed to user authentication and code defects covered 59.8% of the vulnerabilities included in the ICS-CERT advisories after January 1, 2017, i.e., since the FDA postmarket cybersecurity guidance became effective. This seems indicative of a historical way of working in healthcare, wherein the safety burden of a device's operation has been placed on the operator, as opposed to making the device's operation secure by design. This further translates into how software is developed, which is highly reliant on third party libraries, including open source, and not having a plan to mitigate the potential absence of ongoing maintenance by the third party. It is no wonder that post-market vigilance is one of the most commonly called out areas of improvement by the FDA and device consumers. This has been true since we started doing this analysis that year over year, these two are the most frequent drivers for vulnerability disclosures.

Vulnerabilities by Device Type

Advisories tend to focus on specific device classes, like pacemakers, insulin and infusion pumps, and imaging systems (**See Exhibit: 1, below**). Other than those provided by GE and Philips, there is surprisingly an absence of advisories, in particular surgical robots, radiation oncology, and clinical decision support systems.



Relationship Between Device Type and CVSS

We were curious if the clinical intervention a device supported would be reflected in the related CVSS v3 score associated with a vulnerability. As noted in the graph below - more frequent critical vulnerabilities seem to focus around imaging hardware, imaging software, and patient monitoring devices. The imaging-related vulnerabilities are especially interesting as they're unlikely to be characterized as life sustaining devices, but their operation would directly impact the delivery of care.

TYPE OF DEVICECOUNT OF VULNERABILITY DISCLOSURES BY CVSS SEVERITY

	Critical	High	Medium	Low	TM1	Grand Total
Anesthesia			1			1
Bed			1			1
Cardiac Rhythm Management	2	10	15	1	1	29
Diagnostics	4	12	12			28
Drug Dispensing Cabinet		4	4	1	1	10
EKG Analysis Software				1		1
Flow Cytometry			1			1
Imaging Hardware	8	2	3	3		16
Imaging Software	7	22	27	2	1	59
Infusion Pump	4	38	31	2	1	76
Insulin Pump		3	15			18
Network	3	7	1			11
Patient Monitor	6	7	30	4		47
Radiation Workflow	1	1				2
Workflow			2			2
Other	24	34	59	14		131
Grand Total	59	140	202	28	4	433

EXHIBIT 2: COUNT OF VULNERABILITY DISCLOSURES FOR DEVICE TYPES BY CVSS SEVERITY

* Note: line items within an advisory that did not include a detailed CVSS score, had too many CWEs to assess as a collective or did not reference a related CVSS version in scoring (labeled at TM1 in raw data) have been excluded from this analysis.

Vulnerabilities Reach All Time High

Vulnerabilities affecting the Windows OS, hardware components like memory controllers and CPUs, Bluetooth interfaces, and various TCP/IP network stacks have been publicly disclosed, all of which are readily used across the healthcare ecosystem. In 2024 alone, we observed a new all-time high of [over 50,000 vulnerabilities being submitted to the NVD](#).

We hypothesized that the quantity of vulnerabilities attributed to deeply embedded supply chain vulnerabilities would result in a commensurate increase in device or technology-specific disclosures by MDMs. However, we found **no demonstrated impact** of broad impact vulnerabilities on ICS-CERT advisories. In particular, since 2022 there have been no references to third party libraries or encryption tools in vulnerability disclosures reviewed.

This is not to say that MDMs did not disclose such pervasive vulnerabilities, just that the ICS-CERT process is not what was used to do so **(See exhibit: 3, on next page)**.

Vulnerability Frequency vs. ICS-CERT ID Year

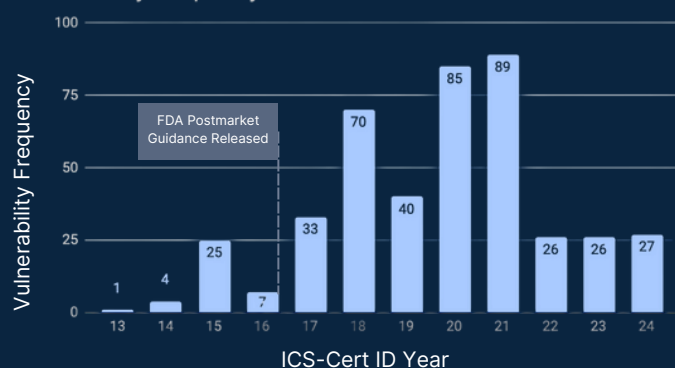


EXHIBIT 3: VULNERABILITY FREQUENCY .> ICS-CERT ID YEAR

Vulnerabilities Reach All Time High

Comparing the list of companies who have made disclosures against a list of device vendors ranked by market cap, of the top 40 medical device vendors, 27 have some communication published around a vulnerability disclosure process. This ranges from fully defined processes including both a mechanism to intake feedback and communicate findings, to an email link. While 31 of the top medical technology vendors have connected devices in their portfolio, 26 have never made a disclosure through ICS-CERT. We would expect that companies with more mature vulnerability disclosure programs would have a greater number of vulnerabilities, as indicated by the fact that nearly half (200/433) of vulnerabilities come from four companies alone (Baxter, BD, Medtronic, and Philips).

There are at least three plausible explanations for why a medical device vendor wouldn't have issued an ICS-CERT disclosure.

1. The device is not connected. Of the top 40 medical device vendors 9 do not offer products that are computerized or connected to a health system network.
2. Communication of the vulnerability and/or fix wasn't made public. There is no law or regulation that states that MDMs must disclose vulnerabilities publicly (unless subject to regulatory recall, corrective action, or removal) therefore it is reasonable to assume that some MDMs simply contact their customers directly rather than putting out full public disclosures.

Of those 27 manufacturers with disclosure processes, 13 have not made a vulnerability disclosure through the ICS-CERT database. We consider the existence of a disclosure policy the "crawl" step of a maturing process. This provides a welcome to researchers and processes internally for receiving a vulnerability report from an external source. Having a disclosure policy is positive for healthcare security, even if it has not yet been used.

That being said, the National Vulnerability Database is another mechanism that is being used as another way for device manufacturers to communicate newly discovered vulnerabilities. However, since NVD is a repository for all software vulnerabilities, it becomes challenging to discern the specific medical device ones. For example, in 2024 alone more than 50,000 new vulnerabilities were recorded in NVD.

We reviewed and contrasted ICS-CERT vs. NVD vulnerability reporting and found some common themes on how manufacturers use these 2 different channels as well as what their respective benefits are, see Appendix D for details.

3. They have never been made aware of or discovered a vulnerability.

Vendors who have yet to issue an advisory due to lack of vulnerabilities should continue to evolve their product development processes including methods for evaluating flaws in architecture and implementation, as well as postmarket monitoring. While internal processes and resources are maturing it may be helpful for MDMs to engage with external resources that specialize in vulnerability discovery and management.

1 This analysis did not comprehensively look at MDM product security website communications

Role of Researchers

Of the 161 advisories assessed, 110 (68%) explicitly referenced a researcher² being involved in the identification of the vulnerability. Historically, researchers have been viewed as adversaries, but their attribution in a majority of advisories confirms their persistent presence in the ecosystem. We believe the presence of researchers impacts patching and data shows that 66.7% of advisories mitigated include reference to a researcher.

RESEARCHER EXPLICITLY REFERENCED	POST - FDA Guidance Release ³	PRE - FDA Guidance Release	GRAND TOTAL
No	50	1	50
Yes	99	11	110
Grand Total	149	12	161

EXHIBIT 4: COUNT OF RESEARCHER REFERENCES IN ADVISORIES

22% Decrease in Advisories Address Patching

Section 524B of the Food, Drugs and Cosmetics Act requires timely patch or update actions be taken to address vulnerabilities on a regular cycle or as soon as possible out of cycle, yet we saw a decrease in advisories including patching references in 2024 by 22% (69% in 2024, compared to 90% in 2023).

While 107 advisories made mention of patching in their original publication, only 19 had multiple revisions - likely associated with patching updates. This could indicate that most advisories notifying that an MDM is planning to patch are not published until a patch is available. Where no mention of a patch was made, only three out of a total 54 advisories issued from 2017-2024 were updated to reference a patch.

CVSS v3.1 enables users to calculate a base score using factors such as attack vector, attack complexity, required privileges, user interaction, scope, confidentiality, integrity and availability. In plotting vulnerability disclosures to date against frequency of patching as a mitigation, there was no statistically significant relationship that could be determined.

Although notable efforts exist to gain visibility into patch availability, implementation, and risk management in a clinical setting, so far they have been idiosyncratic. HDO's patch management is largely reactive and process-driven (e.g., depending on vulnerability disclosure and patch distribution), or limited to addressing the problem "on the outside" through network-based anomaly detection solutions. Certainly, this is a worthwhile effort but it is still limited in effectiveness and impact.

Currently, there are significant barriers to implementing patches in the HDO, when they're available from the MDM. A major barrier is that the device may be in use for extended periods, or that the device is actually updated physically by the staff of the MDM. Both of these issues could contribute to significant delays between disclosure, patch issue, and patch implementation. Unfortunately, the timeliness of patching couldn't be evaluated with the ICS-CERT data set. Does this reactive approach provide a sufficiently secure state across the industry? It's reasonable to assume that we won't be able to patch fast enough and completely enough to become secure enough and therefore, as an industry, need to shift to a more proactive security approach.

² Note - this is not meant to imply that researchers were not involved in other ICS-CERT vulnerability disclosures, only that researchers were explicitly referenced in 11 advisories prior to FDA guidance and 99 since the guidance was issued.

³ FDA Postmarket Cybersecurity Guidance

SECTION III: CONCLUSIONS & PREDICTIONS

It is tempting to draw further conclusions from the data but we do need to recognize that, especially when filtering for certain subsets, the analysis may be skewed by outliers. However, based on the analysis performed as well as our experience in the industry we do want to share a number of hypotheses and predictions that may be of interest for further observation.

HYPOTHESIS



Vulnerability disclosures have reached a plateau and without additional steps by regulators or device consumers, may never mature beyond the current level.



At the current pace of cyber risk evolution, today's security processes/approaches/strategies will remain challenged.



524B of the FD&C Act requires timely patch or update actions be taken to address vulnerabilities on a regular cycle or as soon as possible out of cycle. Yet we still saw a decrease in advisories recommending patching.



Manufacturers are not incentivized to use the ICS-CERT as part of the disclosure process, with pervasive vulnerabilities serving as an example of not having done so. We believe that unless an ICS-CERT is somehow supportive/additive to a resolution, it is unlikely to be published.

MEDCRYPT VIEW



ICS-CERT disclosures are perceived as an after action communication with limited usability for consumers of medical devices. A meaningful change in device market readiness dynamics will need to occur to prioritize security for all stakeholder acceptance. And do so earlier in the development cycle.



We have not made sufficient progress in the last 5 years to change the balance in favor of defenders. A fundamental approach shift to be more proactive/earlier in the supply chain must be adopted for widespread impact.



Statutory authority exists to make change, but we are seeing the pace of enforcement limit the industry's willingness to change.



As cybersecurity matures and manufacturers are able to patch more efficiently and effectively, there will be less of a need for vulnerabilities to be disclosed via the ICS-CERT process.

DISCLOSURES

The authors of this paper are employed by Medcrypt Inc, provider of proactive cybersecurity product and services for medical devices.

APPENDIX A - DETAILED DATA DESCRIPTION

Vulnerability Disclosure Frequency

OCTOBER 2013 TO
DECEMBER 2016

JANUARY 2017 TO
DECEMBER 2021

Number of Advisories	12	149
Total Vulnerabilities Disclosed in Advisories	37	396
Average Advisories per month	0.31	1.55
Average Vulnerabilities per month	0.95	4.125
Companies (advisories issued)	Animas, Baxter, Carefusion (2), Hospira (5), Philips (2), Smiths Medical	Abbott Laboratories, B. Braun, Baxter, Beacon Medaes, Becton, Dickinson and Company (BD), BIOTRONIK, Capsule Technologies, CareFusion, Carestream, Change Healthcare, Dräger, Wind River, Ethicon Endo-Surgery / Johnson & Johnson, Fresenius Kabi, GE, Hamilton Medical AG, Hillrom, Hospira, i-SENS, Innokas Yhtymä Oy, LifePoint Informatics, Medtronic, MicroDicom, Natus Medical, Inc., OFFIS, OpenClinic GA, Orthanc, Philips, Qualcomm Life, Roche, Santesoft, Siemens, Silex, Technology, GE Healthcare, Smiths Medical, Softneta, SOOIL Developments Co., Ltd., Spacelabs, St. Jude, Stryker, Swisslog Healthcare, Vyair, Ypsomed, Zoll
Mean Vulnerabilities' CVSS Score	7.30	6.78 ⁴

EXHIBIT 5: VULNERABILITY DISCLOSURE FREQUENCY

4 FDA Postmarket Cybersecurity Guidance

Advisory Frequency vs. ICS-CERT ID Year

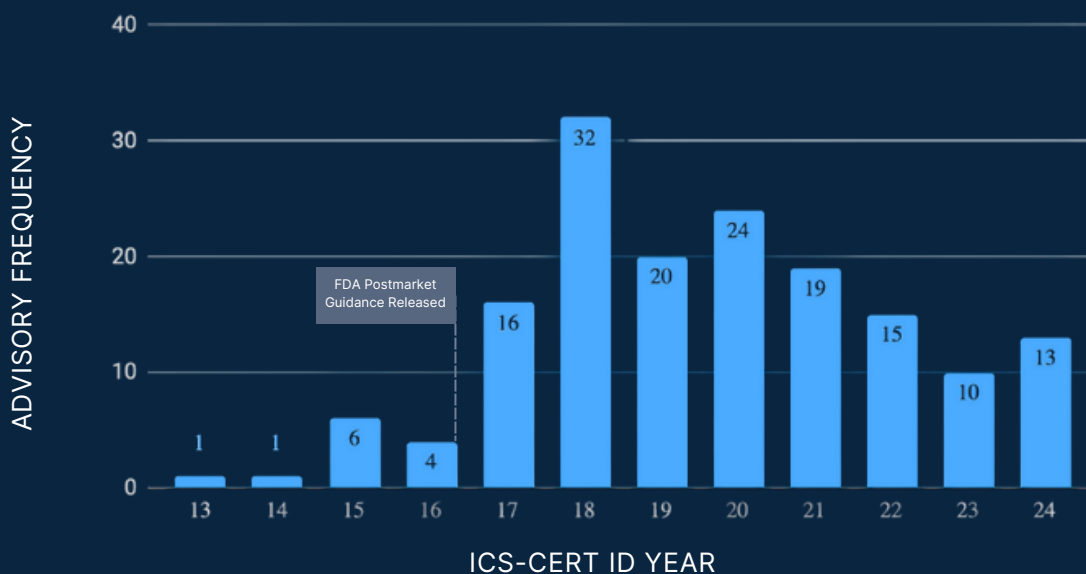


EXHIBIT 6: ADVISORY FREQUENCY BY YEAR

Vulnerability Frequency vs. ICS-CERT ID Year



EXHIBIT 7: VULNERABILITY FREQUENCY BY YEAR

Despite not mandated by law, the number of published vulnerabilities has increased since the release of the FDA Postmarket Guidance, with an average of 4.125 vulnerabilities being released per month, compared to 0.95 per month prior to December 2016. Specifically, applying the National Vulnerability Database (NVD) criteria, details of which are included in [Appendix B](#), the severity of vulnerabilities were expressed as a percentage of the total vulnerabilities disclosed for a time period, as noted in the graphic below.

The timing of FDA guidance demonstrates a pivot point after which there was a large increase in high and medium risk disclosures, along with a decrease in low risk vulnerabilities disclosed. This is particularly impressive since there is no specific disclosure law for MDMs, which means that medical device manufacturers (MDMs) view guidance and other [factors](#) as market incentives.

Pre - FDA and Post - FDA

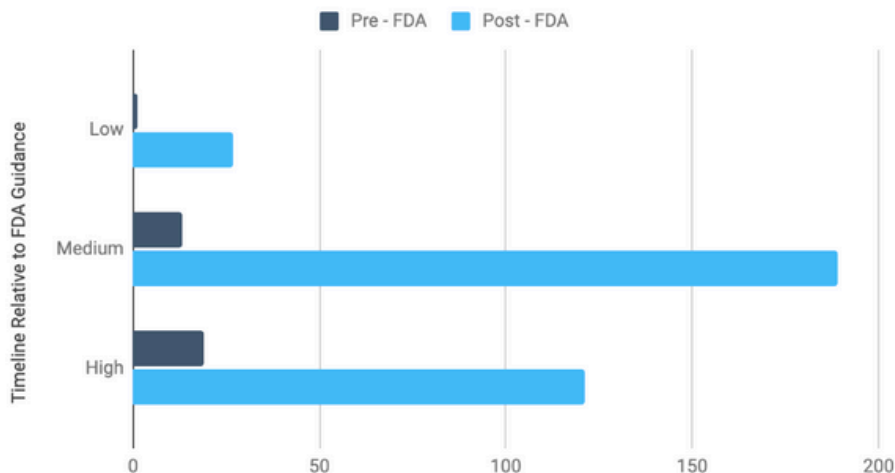


EXHIBIT 8⁵: TIMELINE TO FDA GUIDANCE

Note - those advisories which did not include a detailed CVSS score breakdown or did not reference a related CVSS version in scoring were excluded from analysis.

Vulnerability Causes

We attempted to sort the disclosures into eight categories of technological root causes. While many of the vulnerabilities have aspects of multiple categories, we've matched each common weakness enumeration (CWE) (or common vulnerability exposure (CVE) if a CWE was not referenced in the advisory) with one category. (Please see [Appendix C](#) for an explanation of each category).

ATTRIBUTED ROOT CAUSE	OCTOBER 2013- DECEMBER 2016 TOTALS	JANUARY 2017- DECEMBER 2024 TOTALS
Code Defect	5	72
Encryption	8	49
Operating System Vulnerability	1	28
System Configuration	4	57
Third Party Library	3	10
User Authentication	16	166
Misc	0	12
Grand Total	37	396

EXHIBIT 9: VULNERABILITY ROOT CAUSE

Role of Security Researchers

Since the first medical device security researcher shared their findings, the role of security researchers in healthcare cybersecurity has continued to evolve. While there are stories of researcher's work that have splashed across mainstream media headlines, the medical device community at large, including regulators, has gone through great efforts to build a trusted and collaborative relationship between researchers and device manufacturers. 2024 is great evidence of this, as there was a near doubling of researcher references in advisories compared to 2023.

RESEARCHER EXPLICITLY REFERENCED	POST - FDA	PRE - FDA	GRAND TOTAL
No	50	1	51
Yes	99	11	110
Grand Total	149	12	161

EXHIBIT 10: RESEARCHER EXPLICITLY REFERENCED

Correlation of CVSS to Root Cause

CVSS scores can draw a visceral response from the healthcare industry because CVSS scores are an approximation of risk, but in practice they often don't correlate well with realized risk, exploitability etc. Conceptually, CVSS can help prioritize mitigations by incorporating exploitability risk factors into overall decision making, and FDA recommends the use of CVSS in their postmarket guidance. .

ROOT CAUSE	TIMELINE RELATIVE TO FDA GUIDANCE ⁷	
	POST - FDA	PRE - FDA
Code Defect	6.7	7.6
Encryption	6.3	6.4
Misc	5.1	0
Operating System Vulnerability	7.05	7.0
System Configuration	6.5	7.5
Third Party (Encryption)	5.9	0
Third Party Library	7.9	8.4
User Authentication	7.05	8.1

EXHIBIT 11: MEDIAN CVSS VALUE

6 When looking at trending CVSS scores or comparison of CVSS scores across categories we can choose statistical methods that describe a central or representative value of a group of numbers. The Median has been assessed as it is the preferred measure when describing data sets that are skewed or contain significant outliers.

7 FDA Postmarket Cybersecurity Guidance

Patching as a Mitigation

Currently, disclosure is a complex mechanism for information sharing to enable risk reduction. Even without a patch or fix, disclosure by technology builders is seen as helping consumers defend against attackers. While there are complications in the healthcare space with respect to patching, patching is seen as a robust risk-reducing method. Since 2016, when the FDA postmarket guidance emphasized the importance of patching, the number of disclosed advisories that received a patch increased by 1.5x - with 77.3% of advisories being patched since post-guidance publication (See Exhibit: 12).

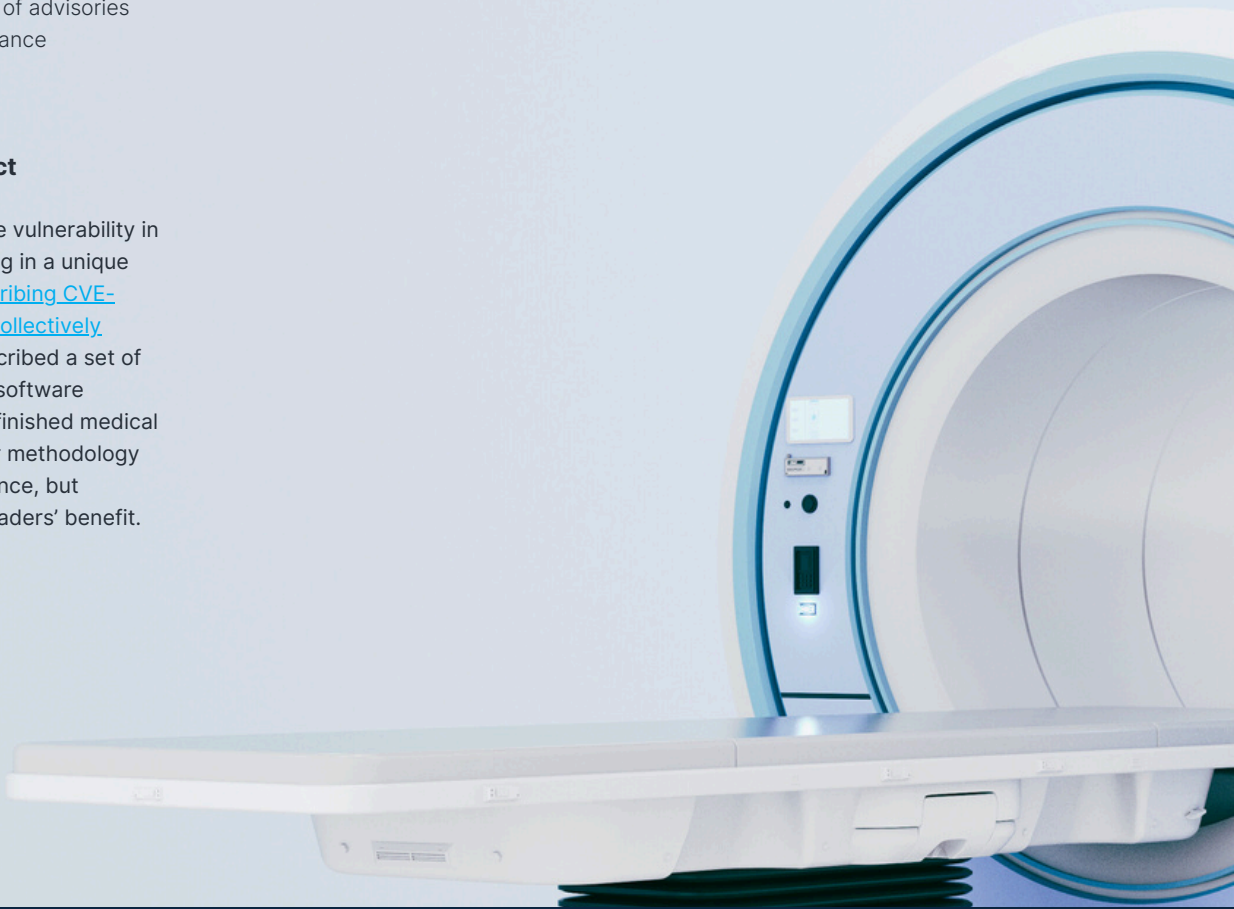
Prevalence of broad impact vulnerabilities

Please note that there was one vulnerability in 2019 that stood out as resulting in a unique advisory, [JCSMA 19-274 \(describing CVE-2019-12256 through -12265, collectively known as Urgent/11\)](#), as it described a set of vulnerabilities of a third party software product rather than an actual finished medical device. We did not change our methodology because of this single occurrence, but wanted to clarify this to the readers' benefit.

Advisories that list patching as a mitigation

	NO	YES
No	90	305
Yes	18	19
Grand Total	108	324

EXHIBIT 12: ADVISORIES THAT LIST PATCHING AS A MITIGATION



Medcrypt provides proactive security for healthcare technology. Medcrypt’s platform brings core cybersecurity features to medical devices with just a few lines of code, ensuring devices are secure by design. As of today, Medcrypt has secured a total of \$36.4 million in funding, with investments from notable entities such as Intuitive Ventures, Johnson & Johnson Innovation – JJDC, Inc., and Dexcom Ventures. The company announced a \$5.3 million Series A funding round in May of 2019, bringing the total funds raised at the time to \$9.4 million, with participation from Eniac Ventures, Section 32, Y Combinator, and more. Medcrypt is based in San Diego, California.

For further details, please visit and contact:

- Website: www.medcrypt.com
- Email: info@medcrypt.com
- X: [@Medcrypt](#)
- Bluesky: [medcrypt.bsky.social](#)

APPENDIX B

The advisories under review were bucketed into qualitative ranges based on the NVD criteria. Where a version of CVSS was not referenced or hundreds of vulnerabilities were included in a single advisory (see TM1 in raw data), these were excluded from the assessment. (See Exhibit: 13).

TIMELINE RELATIVE TO FDA GUIDANCE

	HIGH	MEDIUM	LOW	TM1	GRAND TOTAL
Post - FDA ⁸	121	27	189	1	396
Pre - FDA	19	1	13	3	37
Grand Total	140	28	202	4	433

EXHIBIT 13: TIMELINE RELATIVE TO FDA GUIDANCE

The transition to CVSS4.0 will present opportunities and challenges - as 4.0 consolidates the threat metric group, eliminating redundancies and refinement to the attack complexity metric. This should result in a more streamlined scoring system and improved clarity.

Qualitative Severity Rating

CVSS v2.0 Ratings		CVSS v3.x Ratings		CVSS v4.0 Ratings	
Severity	Severity Score Range	Severity	Severity Score Range	Severity	Severity Score Range
		None*	0.0	None*	0.0
Low	0.0-3.9	Low	0.1-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9	High	7.0-8.9
		Critical	9.0-10.0	Critical	9.0-10.0

EXHIBIT 14: QUALITATIVE SEVERITY RATING



APPENDIX C

Description of Vulnerability Cause Categories

Code Defect	Can be described as imperfect implementations of otherwise secure software designs. An example of a code defect would be a Buffer Overflow . Many of these defects can be identified in the verification and validation process using tools like Static Code Analysis and Fuzz Testing.
Encryption	The lack of encryption of sensitive data, or vulnerabilities in the way this encryption is implemented, can leave devices and data vulnerable to attack. Common examples are storing user credentials in plain text, storing encryption keys in an insecure fashion, or vulnerabilities discovered in the underlying encryption software and algorithms.
Operating System Vulnerability	Many medical devices include computers running retail operating systems, like Microsoft Windows. These operating systems are regularly found to have vulnerabilities unrelated to the medical device itself, but that can affect the function of the device if left unpatched. One example would be the March 2017 “EternalBlue” vulnerability in Microsoft Windows handling of SMB transactions.
User Authentication	Failure to require user authentication for critical functions, or vulnerabilities in the way users are authenticated, can leave devices susceptible to attack. One common example is the use of “hard-coded” user credentials used across a fleet of devices.
System Configuration	Connected medical devices and their underlying software systems can be designed “securely”, but configured in a way that leaves a device susceptible to attack. A common example is failing to disable unnecessary OS services and block all unused ports.
Third Party Library	Medical devices frequently rely on third party software for critical functions, which can be found to have vulnerabilities. One example would be a medical device including a version of a database server application found to have a publicly disclosed vulnerability.
Third Party Encryption	Use of a third party hard- or software component that demonstrated a weakness related to its encryption algorithm. (e.g. OpenSSL)
Miscellaneous	Disclosures that did not fit into one of the above categories were labeled “Miscellaneous.”

EXHIBIT 15: Description of Vulnerability Cause Categories



APPENDIX D

The NVD (National Vulnerability Database) and ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) serve different purposes in cybersecurity, although both contribute to protecting critical systems and networks.

	ICS-CERT	NVD
Purpose and Scope	• Focuses on vulnerability advisories specifically related to industrial control systems (ICS), operational technology (OT), and critical infrastructure sectors (e.g., energy, water, transportation). This includes advisories specific to medical devices. • Emphasizes maintaining operational safety while addressing vulnerabilities.	• Provides a comprehensive, public-facing database for vulnerabilities across a wide range of software and hardware products, including IT systems. • Broader in scope, supporting the general public, researchers, and organizations in identifying Common Vulnerabilities and Exposures (CVEs).
Audience	• Primarily targets industrial organizations and stakeholders involved in critical infrastructure sectors, including healthcare. • Collaborates with vendors, asset owners, and government agencies to address ICS-specific vulnerabilities.	• Serves a wider audience, including developers, IT administrators, researchers, and the general public. • Is, to date, the only non-commercial, comprehensive database of software vulnerabilities and is used internationally.
Disclosure Process	• Coordinated Disclosure: ◦ Works with vendors to verify and remediate vulnerabilities before public disclosure. ◦ Seeks to provide actionable mitigations while minimizing operational risks. ◦ May delay or suppress disclosure if public knowledge could lead to exploitation in critical systems. • Incident Handling: ◦ Emphasizes incident handling and remediation coordination with affected stakeholders. ◦ Produces ICS-CERT Advisories or Alerts, which are often tailored for operational environments.	• Automated and Standardized Process: ◦ Vulnerabilities are submitted by an authorized CVE Numbering Authority (CNA) and are augmented and enriched by NVD personnel. ◦ Relies on CVE records maintained by the MITRE Corporation. Once a vulnerability is assigned a CVE ID and details are published, NVD ingests this data for public access. ◦ Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) to provide an objective measure of severity. • Timeline: ◦ Does not actively engage in vulnerability remediation or coordination before publishing. ◦ Vulnerabilities may appear in NVD even if they are not yet complete and are undergoing an enrichment process . ◦ Starting in early 2024, NVD CVE enrichment/processing has significantly slowed and created a backlog.
Reporting Format	• Produces detailed, operationally focused advisories. ◦ Advisories include background information, risk assessment, affected products, and specific mitigations tailored for ICS environments. ◦ Prioritizes practical recommendations for stakeholders (e.g., patching, network segmentation, or alternative controls).	• Standardized entries for each CVE: ◦ Includes descriptions, severity scores (CVSS), affected products, and references. ◦ Focused on cataloging vulnerabilities rather than providing tailored mitigations.
Risk Scoring and Prioritization	• May adjust risk prioritization based on real-world operational impacts (e.g., safety, availability, and criticality of affected systems).	• Primarily uses CVSS scores for standardized severity ratings. ◦ CVSS considers exploitability and impact but does not always reflect the operational context (e.g., safety implications in critical systems). ◦ The typical CVSS use case is the scoring of a software component in the abstract (i.e., not considering the specific implementation in a system and its use case). However, CVSS is also used to score system-level vulnerabilities, which is an important distinction when interpreting CVSS scores.

Key Takeaway

The NVD (National Vulnerability Database) and ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) serve different purposes in cybersecurity, although both contribute to protecting critical systems and networks.

	ICS-CERT	NVD
Priorities	Prioritizes coordinated disclosure, operational safety, and tailored guidance for critical infrastructure stakeholders. It addresses vulnerabilities in a highly specialized domain where safety and reliability are paramount.	Focuses on broad, public cataloging of vulnerabilities across a wide array of IT products, emphasizing accessibility and standardization.

Both systems serve important but distinct roles, with ICS-CERT tailored for critical infrastructure and NVD catering to the broader IT and software ecosystem.

Contrasting ICS-CERT vs. NVD Vulnerability Disclosure Practical Example

We reviewed a sampling of ICS-CERT medical device vulnerability disclosures and their corresponding NVD entries and tried to discern some patterns that may be useful for both producers as well as consumers of vulnerability disclosure information.

	ICS-CERT	NVD
Common Themes	- Medical device advisories are uniquely numbered (ICSMA) within the larger ICS database. However, before 2015 medical device advisories were numbered as ICSA (same as all ICS advisories). - The numbering has the format ICS-ICSMA yy-<i>nnn</i>-xx with yy denoting the advisory year, <i>nnn</i> being a sequential number. - At first glance it appears that xx would denote updates (which, in some cases it does), however, among our samples we also found examples where xx may refer to different products by the same manufacturer or even, in a few exceptions, to different manufacturers. - A given ICS-CERT advisory may contain 1 or a few (2-3, in exceptional cases 10+) individual vulnerabilities which are listed as individual CVEs and classified by respective CWE categories. - CVEs are typically assigned to vulnerabilities identified within a given product and that are unique to the product, but in some cases may refer to existing general software CVEs for known vulnerabilities of an off-the-shelf (OTS) software component used within the product. - For product-specific vulnerabilities, ICS-CERT acts as a CVE Numbering Authority (CNA) and submits the individual vulnerabilities (1 to several per product) to NVD. - For a few of the ICSMAs that were disclosed in late 2024, ICS-CERT refers to CVE.org instead of NVD. - Each individual vulnerability within an ICSMA advisory refers to a specific CVE in NVD, either for a complete product (in most cases) or to an existing OTS vulnerability. - This may be mixed, i.e., a given ICSMA may contain product-specific and OTS CVEs.	- The quality and completeness of an NVD entry may vary and may have missing elements (including missing manufacturer and/or product names, in some cases there may be no information other than “number reserved”). - NVD may add additional, supplemental information to an individual CVE, e.g., add additional CWEs. - Information typically present in the NVD CVE entry in a set of free description text fields: - Manufacturer name (but has been missing in some cases) - Product name (but has been missing in some cases) - ICSMA number and reference - Additional relevant reference information, e.g., manufacturer web site or software component vulnerability information or device CPE. - CVE description is usually fairly comprehensive but, in some cases, lacks detail, e.g., “Description: The software does not perform any authentication for critical system functionality” (without manufacturer or product nor specific vulnerability information). - The CVSS score assigned to a CVE may vary between ICSMA and NVD, sometimes a little (few tenth) sometimes significant (few points). This may be due to NVD re-scoring the vulnerability when created or that changes over time are not equally maintained between the two sources. - Searching NVD for vulnerabilities provides more or less complete results but some oddities need to be considered: - When searching for a manufacturer, the name may not be listed in the CVE description and therefore will not return the respective CVE as a result. - A CPE may be assigned but due to CPE inconsistencies (that are, unfortunately, present) a search may produce incomplete results. - Searching for specific CPEs may provide incomplete results (missing CVEs), for no apparent reasons (i.e., no obvious spelling error, ...). - ICS-CERT started tracking medical device vulnerabilities in 2013, so an NVD search may identify additional vulnerabilities from 2013 or before.