Medcrypt

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

2026 EDITION | DECEMBER 1, 2026

Reflecting on fourteen years of CISA medical device advisories: who discloses, what breaks, and what's changing.

EXECUTIVE SUMMARY

This edition extends our analysis of CISA ICS medical advisories (ICSMA) through November 13, 2026: **202 advisories and 527 vulnerabilities from 2013 to 2026**, including 42 published since our last edition, which covered through 2024. It uses the same categories as prior editions: root cause, device type, care setting, patching and researcher credit.

AT A GLANCE

0	Manufacturer self-reports to CISA (flaws found in their own testing) in 2025–2026, down from 4–9 a year in 2017–2024
22	Imaging software advisories in 2025–2026, more than half the total
62%	2025–2026 advisories about vendors new to CISA's list
7.8	Median highest CVSS v3 score per advisory in 2025–2026, up from 7.5 in 2021–2024 and 7.1 in 2017–2020
9 of 42	2025–2026 advisories for products used at home
4	2025–2026 advisories published without a response from the vendor or maintainer

Who discloses, and where. Manufacturers stopped reporting flaws found in their own testing to CISA, from 4 to 9 advisories a year in 2017–2024 to none in 2025–2026. Large manufacturers

now publish on their own portals instead. Disclosures haven't stopped, but they have scattered, which makes it harder for hospitals to stay informed. Most new advisories (62%) name a company or project that had never appeared on CISA's list before.

What breaks. Imaging software and open-source DICOM code now lead the list, infusion pumps have dropped off, and about half of all advisories cover software and IT systems used in healthcare, such as imaging archives, integration engines and lab software, rather than devices. Code defects are rising, most flaws can be reached over a network, and CVSS scores are climbing. Fewer advisories come with a fix, and only 3 of 9 patient monitor advisories since 2021 came with a patch.

What's changing. Care is moving home: 9 of the 42 advisories in 2025–2026 cover home-use products. The 2026 enterprise attacks showed what cyber incidents cost device makers, even without a device flaw. And AI is speeding up discovery in ways CISA's list doesn't show yet.

WHAT WE RECOMMEND

Who	What to do
Manufacturers: disclosure	Coordinate a CISA advisory and CVE record, not just a portal notice. Keep a reachable security contact, and publish a support period for every product.
Manufacturers: engineering	Track open-source imaging libraries and AI models in your SBOM, and load models only in safe formats such as safetensors. Design out trust boundary and authentication flaws with threat modeling, and cut code defects with memory-safe languages, secure coding practices, code review, and appropriate testing.
Manufacturers: risk	Use a security risk assessment that includes patient harm under ISO 14971, with CVSS as one input to prioritize, not the final word. Plan for more incoming vulnerability reports as AI tools spread.
Hospitals and buyers	Don't rely on CISA alone for vulnerability notifications. Check each vendor's own portal and SBOM.
Regulators	Treat advisories that CISA published after the vendor didn't respond as a postmarket signal.

SECTION I: DATA

This edition combines Medcrypt's hand-coded assessment of CISA medical advisories from 2013 to 2024 with the same coding applied to every advisory published 2025 through November

13, 2026[1,3]. We count vulnerabilities and roll them up to advisories, and we define large manufacturers as the companies on MDDI's top-40 list[5]. Appendix A has the full method. Year-by-year figures (Figure 1 and Appendix C1) start in 2017, because 2013–2016 had only 12 advisories in total and the large-manufacturer counts begin in 2017. Unless a single year is named, comparisons with our last edition use 2025–2026 (42 advisories, 94 vulnerabilities). An advisory's "vendor" is the company or open-source project it covers, which can be a device manufacturer, a software company or a volunteer project. A manufacturer self-report is an advisory where that vendor found and reported the flaw itself.

A NOTE ON VENDOR NAMES
This edition names manufacturers and open-source projects where CISA's public advisories or the companies' own pages support it. A high count usually reflects a mature disclosure program, not weaker products: companies that look for and report flaws appear more often. Absence from CISA's list is not evidence of security.

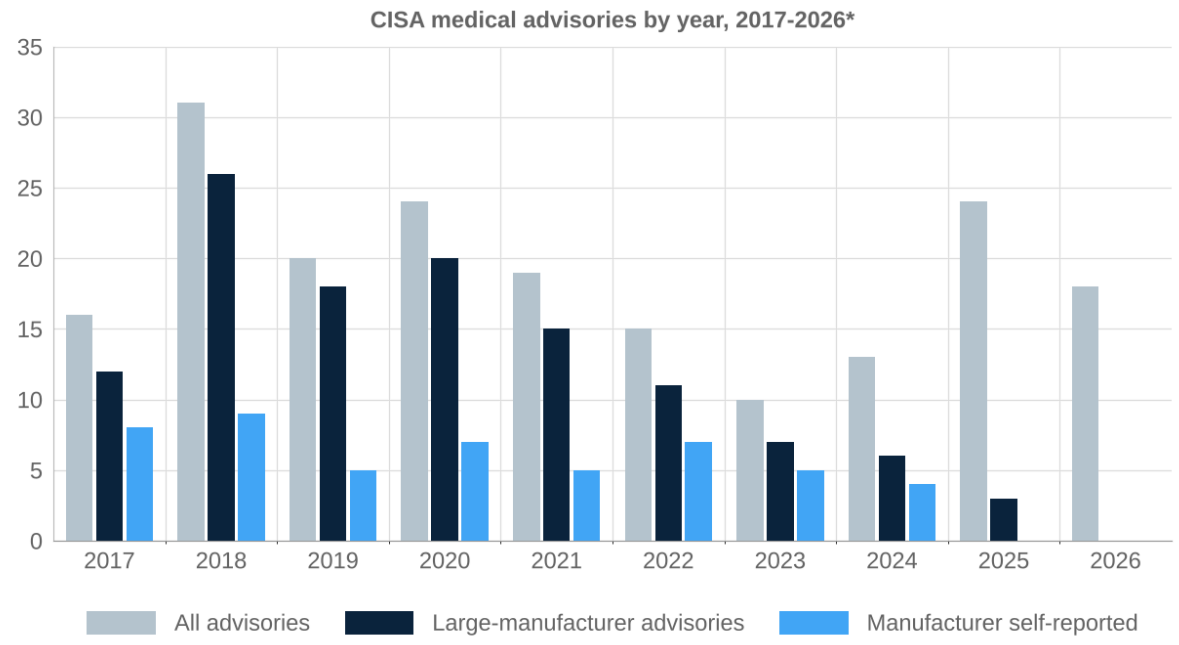

Figure 1. CISA medical advisories by year, 2017–2026 (2026 through November 13). Large-manufacturer counts for 2017–2024 follow Kijewski (2026).

SECTION II: OBSERVATIONS FROM THE DATA

PART 1: WHO DISCLOSES, AND WHERE

MANUFACTURERS STOPPED SELF-REPORTING TO CISA

In every year from 2017 to 2024, some advisories credited no outside researcher: the manufacturer found and reported the flaw itself. BD did this every year. Philips, Baxter, Medtronic and others did it in several years. In 2025 and 2026, all 42 advisories credit an outside researcher or organization. Those findings still reach CISA with the vendor coordinating; what stopped is manufacturers reporting flaws from their own testing.

The vendors that disclosed the most are the ones that left CISA's list. Philips, BD, Baxter and Medtronic account for 206 of the 527 vulnerabilities in CISA medical advisories since 2013 (Figure 2), but most of those were disclosed before 2023. Their absence from the 2025–2026 list reflects where they now disclose, not how secure their products are.

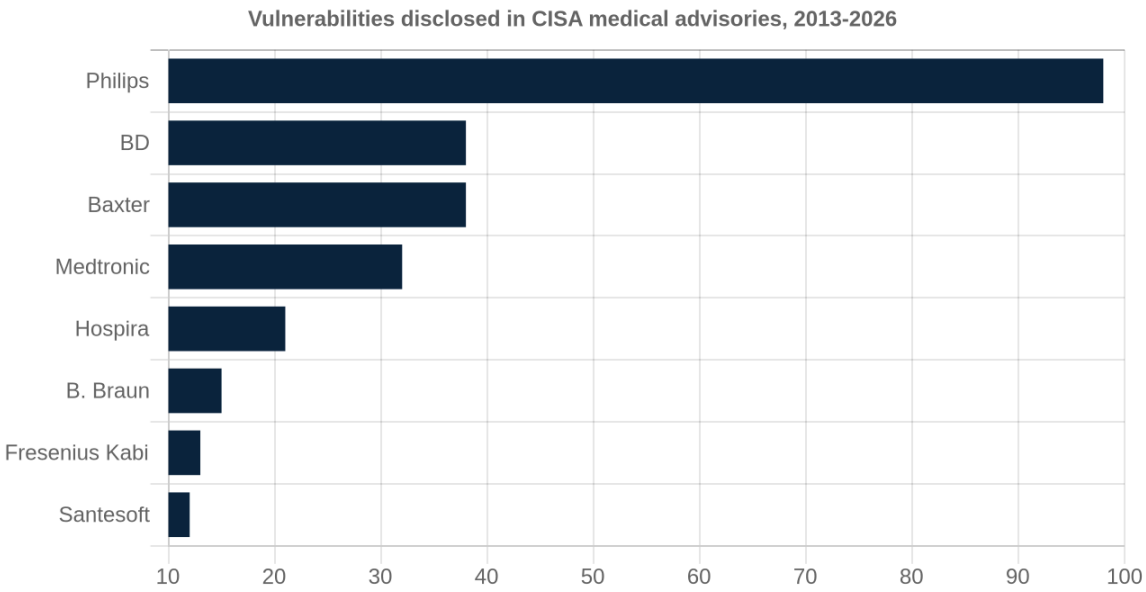

Figure 2. Vulnerabilities in CISA medical advisories by vendor, 2013–2026 (top eight).

DISCLOSURE SCATTERED TO COMPANY PORTALS

CISA's list now captures less of what large manufacturers disclose. Medtronic's security bulletins page lists a CareLink Network bulletin (December 2025, updated January 2026) with no matching CISA advisory. Philips posted 29 notices on its 2026 advisory page; one references a CISA advisory (Mirth Connect), and most cover third-party software such as Windows and open-source libraries, or outside incidents, rather than flaws in Philips code. BD, an authorized

CVE Numbering Authority, publishes its own bulletins and patch pages. Our review of all 40 top manufacturers' portals, below, found the same pattern.

For hospitals, this is a step back. A CISA advisory reaches every subscriber in one standard format. Portal notices don't. A hospital security team now has to watch each manufacturer's page, in that manufacturer's format, to learn about flaws in devices already on its network, and most hospitals run equipment from dozens of manufacturers.

PROGRAMS HELD STEADY, AND THE ATTACKS DIDN'T CHANGE THEM

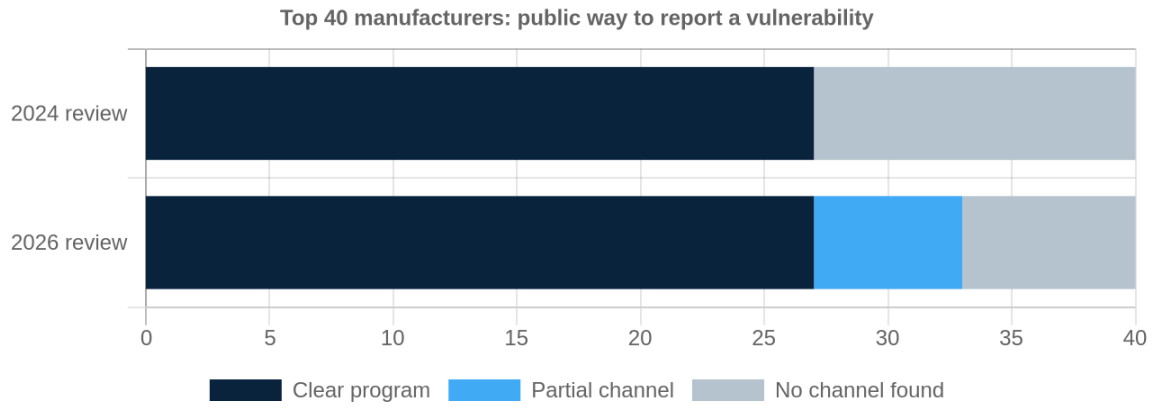

Figure 3. Top 40 manufacturers with a public way to report a vulnerability, 2024 vs. 2026 (reviewed November 16, 2026). The 2024 review didn't separate partial channels.

The number of top-40 manufacturers with a clear way to report a vulnerability held at 27 of 40[6]. Six more now have a partial channel, such as a security.txt file or a page with no contact, so the number with nothing fell from 13 to 7. Six are confirmed CVE Numbering Authorities (Medtronic, BD, GE HealthCare, Philips, Baxter and Hologic), plus Radiometer under Danaher.

Five programs got stronger and two got weaker since 2024, and several companies' advisory lists have gone stale (Appendix C has the details).

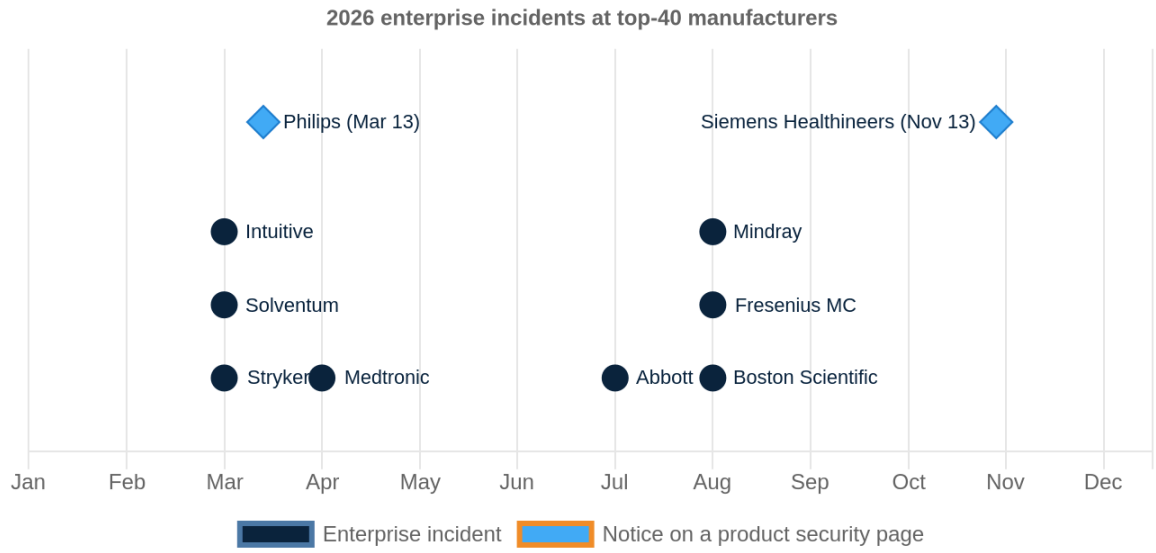

Figure 4. 2026 enterprise incidents at top-40 manufacturers, and the only two related notices on product security pages.

At least eight of the top 40 had enterprise incidents in 2026. Each communicated through newsroom statements, incident pages, customer letters or SEC filings, and nearly all stressed that devices and patients were unaffected. Only two touched their product security pages: Philips now posts enterprise incidents in its product security feed, including a notice about the Stryker attack (March 13), and Siemens Healthineers posted a Microsoft 365 disruption notice (November 13).

PART 2: WHAT BREAKS

IMAGING SOFTWARE TOOK OVER

Imaging software went from 2 advisories in 2013–2016 to 22 in 2025–2026, while patient monitors and cardiac rhythm devices faded from the list (Figure 5). The reasons are structural, and they don't mean imaging vendors are more careless than anyone else.

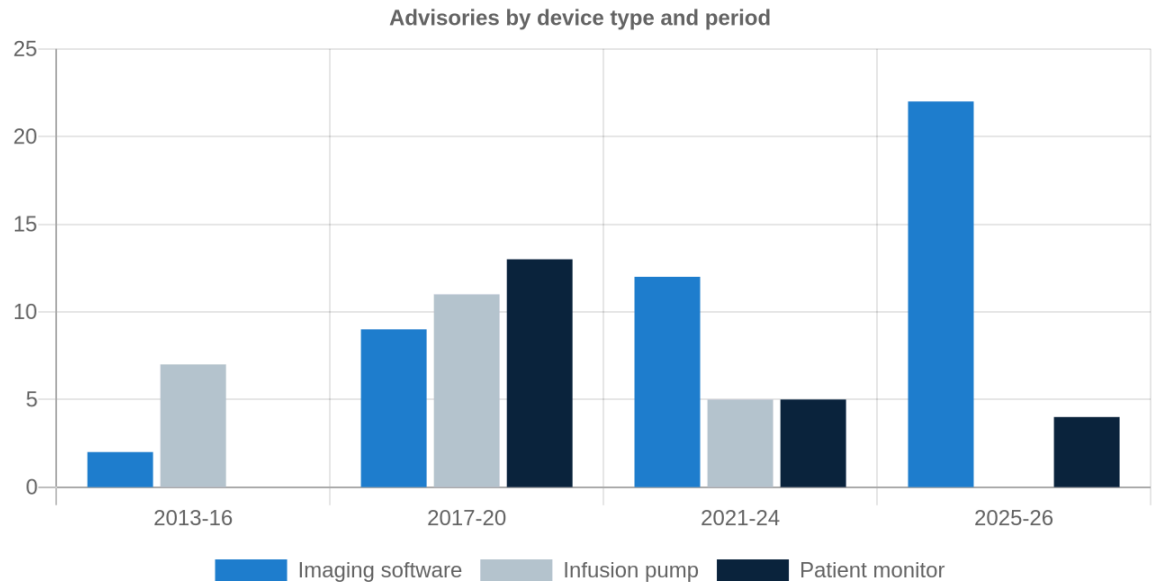

Figure 5. Advisories by device type and period. Source: Medcrypt analysis of CISA ICSMA advisories.

The standard was built for sharing. DICOM dates to the early 1990s, when imaging moved onto hospital networks, and its job is to move images between scanners, archives and viewers from different vendors. Authentication and encryption exist as optional profiles that many deployments don't turn on, so an imaging server will often answer anyone who can reach it.

DICOM libraries are complex, and files arrive by many routes. A DICOM file can carry hundreds of data elements, nested sequences, compressed pixel data and vendor-specific private fields. Viewers have to open these files from CDs, email, patient portals and other hospitals, which is exactly the kind of untrusted input where memory-corruption and path-traversal bugs show up.

The code is shared. A handful of open-source toolkits, such as DCMTK, GDCM, dcm4che and pydicom, sit inside many commercial viewers and archives, often maintained by small teams. One flaw reaches every product that embeds the library, and a manufacturer that doesn't track the library in its SBOM may not know it's exposed. And when a researcher reports a flaw in one of these libraries, the maintainer may fix it, but there is no defined path for that fix to reach the finished products built on it.

Much of it sits outside traditional device programs. Many viewers are free downloads or standalone software used by clinicians and patients, often from small vendors without a disclosure program. Imaging archives stay in service for years, and updates often mean revalidation and downtime, so fixes arrive slowly even when they exist.

OPEN SOURCE IS NOW PART OF THE DEVICE SUPPLY CHAIN
Six open-source DICOM projects accounted for 8 CISA medical advisories in 2025–2026, and in two of them, GDCM and pynetdicom, CISA published without hearing back from the maintainers. That isn't negligence. These projects are often run by a few people, sometimes volunteers, with no contract obliging them to fix anything on a manufacturer's schedule. Yet their code sits inside commercial viewers, archives and AI pipelines that carry FDA obligations. The risk transfers to the manufacturer whether or not its SBOM lists the library: when an upstream fix is slow or never comes, the manufacturer still owns the patch, the mitigation and the postmarket report. The same pattern is now reaching AI frameworks such as MONAI.

ROOT CAUSES: CODE DEFECTS ARE RISING

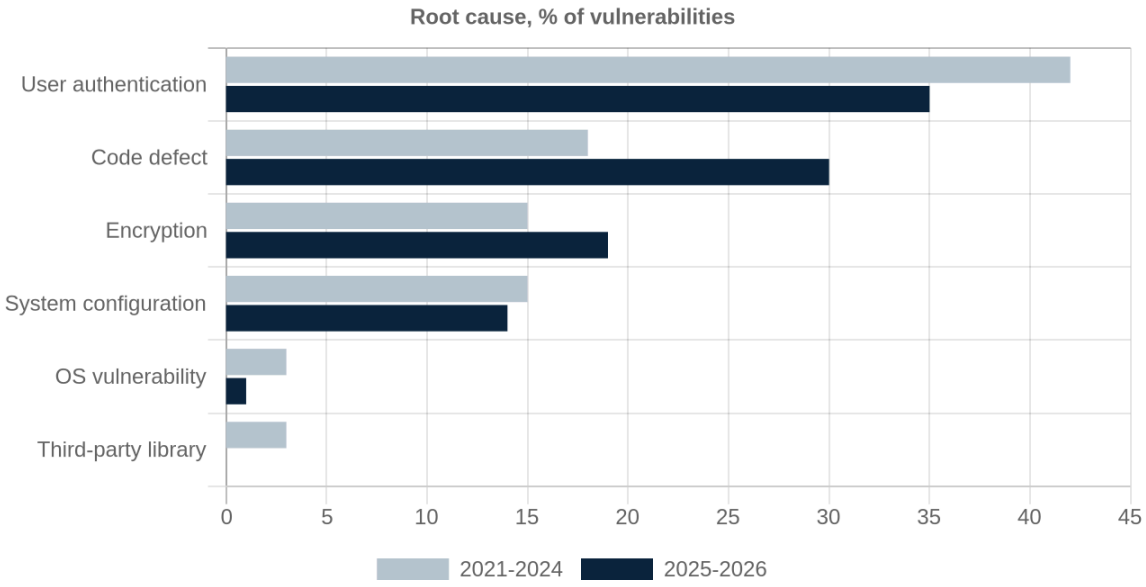

Figure 6. Root cause, share of vulnerabilities, 2021–2024 vs. 2025–2026. Source: Medcrypt analysis of CISA ICSMA advisories.

Advisories against open-source libraries are coded as code defects in the library itself. For a manufacturer that ships the library, the same flaw is a third-party library issue.

SEVERITY IS RISING

The median highest CVSS v3 score per advisory rose from 7.1 in 2017–2020 to 7.5 in 2021–2024 and 7.8 in 2025–2026 (8.15 in 2026 alone). 14 of 2026's 18 advisories are High or Critical, and 5 are Critical, up from 3 in 2025.

The rise is a real signal. CVSS is the common language of suppliers, CISA and FDA, and its exploitability metrics show a clear shift: 62% of 2025–2026 vulnerabilities can be exploited over a network, and 79% need no privileges. More flaws are easy to reach, and more would do serious damage to the systems they sit in.

What CVSS can't tell you is what a flaw means for patients. As we argued in "CVSS for Medical Device Product Risk: Flawed, but Still Essential,"[7] CVSS was built to give an abstracted severity score for enterprise IT, and it rates impact on data, not on care. None of the CVSS v4 vectors CISA published for 2025–2026 sets v4's optional Safety metric, and none of the 2025–2026 CVEs is on CISA's Known Exploited Vulnerabilities list yet[2]. Use the score to prioritize, and the manufacturer's ISO 14971 assessment to judge patient risk.

FEWER ADVISORIES COME WITH A FIX

67% of 2026 advisories include a patch or update, down from 83% in 2025. The gap has two sources. Some advisories went out without any response from the vendor or maintainer, after CISA's attempts to coordinate went unanswered: BPL Medical Technologies in 2024, Qardio in 2025, and Apollo Pharmacy and the GDCM and pynetdicom projects in 2026, something that hadn't happened before 2024. Others had already ended support, so the advisory came with an end-of-life notice instead of an update: Panoramic's imaging SDK (2025), older Thermo Fisher genetic analyzers (2026) and ZOLL's decommissioned ePCR iOS app (2026). Either way, hospitals are left managing the risk with network controls instead of a fix.

Device type matters more than who found the flaw. Since 2021, imaging software had a patch available 88% of the time, infusion pumps 80% and diagnostics 71%, while only 3 of 9 patient monitor advisories did (Figure 7). Who found the flaw makes a smaller difference (Appendix C2).

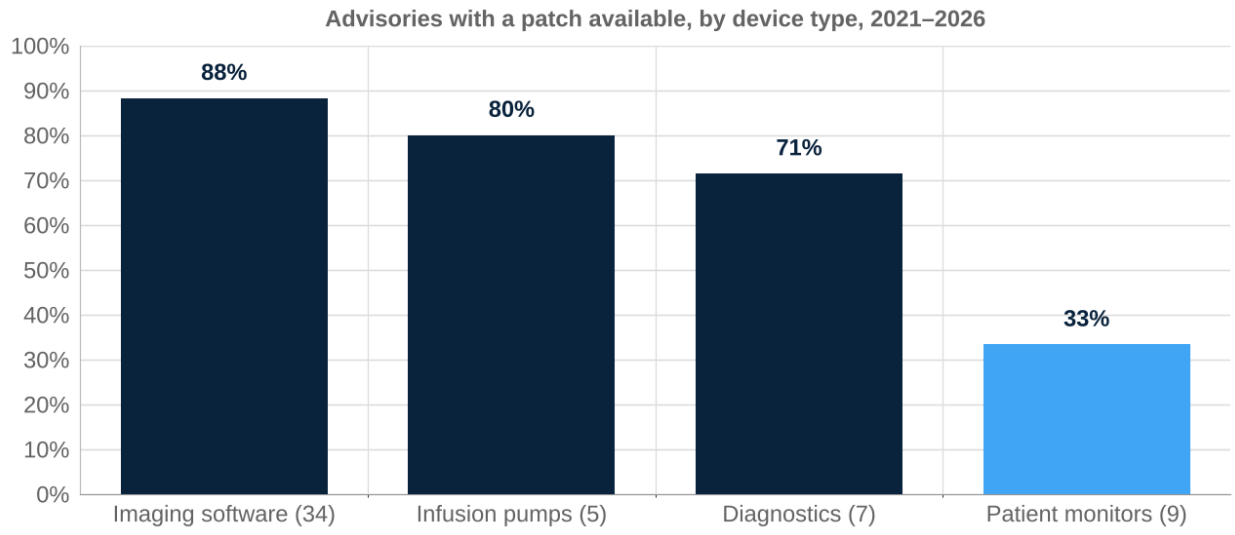

Figure 7. Share of advisories with a patch available, by device type, 2021–2026 (number of advisories in parentheses).

PART 3: WHAT'S CHANGING

WHAT THE ENTERPRISE ATTACKS COST, AND WHY PRODUCT SECURITY SHOULD CARE

None of 2026's enterprise attacks started with a device vulnerability, and every company that was hit said its products were unaffected. The bills still landed. Boston Scientific's August attack cut about $150 million from third-quarter revenue, and the company expects another 200 to 300 basis points of drag in the fourth quarter. Stryker paused manufacturing for about three weeks after its March attack, called the hit to its first quarter material, and now faces a securities class action. Medtronic's April incident didn't affect devices either, but the company still had to notify 3.8 million patients whose personal and medical data was impacted[8].

For product security teams, these numbers are a preview. The systems that build and support devices sit inside the same enterprise: build pipelines, code-signing keys, update servers and service tools. An outage that stops manufacturing can also stall patches and field service, and a compromised signing key or update channel would turn an IT incident into a product one. The assurance each company gave customers, that product networks were separate and devices unaffected, is only as strong as the evidence behind it. Section 524B and FDA's premarket guidance already ask for that evidence (SBOMs, architecture views and postmarket plans), and QMSR inspections now check it.

A device-level incident would also bring costs these attacks didn't: cybersecurity recalls, which already happen (Abiomed's Impella controller in 2025, and GE HealthCare's Centricity Universal Viewer and AW Server in 2026), FDA reporting and patient-safety exposure. And customers can least afford the spillover. Mike Kijewski's analysis, recently presented at UC San Diego, estimates[4] that healthcare loses about 13.3% of profit to cyber incidents, against 0.7% in financial services, on an average hospital margin of 4.9%. Hospitals will increasingly ask device makers to show, not just say, that products are isolated from enterprise risk.

AI IS CHANGING WHO FINDS FLAWS, AND WHAT COUNTS AS A COMPONENT

CISA's acknowledgments don't record how a flaw was found, so we can't measure AI's contribution directly. But four patterns in the 2025–2026 data match what AI-assisted discovery is doing across software.

5 of 18
2026 advisories credited to a single researcher

~8%
of findings disclosed through Project Glasswing patched by October 2026

~1 day
from *sshole's fix to attacks in the wild

0 of 42
2025–2026 CISA medical advisories that involve an AI component

A few researchers cover a lot of ground. One researcher is credited on 5 of 2026's 18 advisories, across DCMTK, Mirth Connect, Torrent Suite, dcm4che and IRIS for Health. Another had 4 in 2025. Sweeps across open-source code like this are what source-review tools, including AI, make cheap.

Maintainers can't keep up. Across software, partners in Anthropic's Project Glasswing reported at least 129,000 verified vulnerabilities from April to July 2026[9], and only about 8% of disclosed findings were patched by October. curl, Google and the Internet Bug Bounty ended or paused bug bounty programs over the volume.

Shared components get hit without a medical advisory. *sshole (CVE-2026-123158), found with what its discoverer calls "agent swarms,"[11] lets attackers log in to locked accounts on OpenSSH running on musl-based Linux, including Yocto and Buildroot builds common in embedded devices. The bug dates to 2012, attackers exploited it about a day after the November 5 fix, and there is no CISA medical advisory for it.

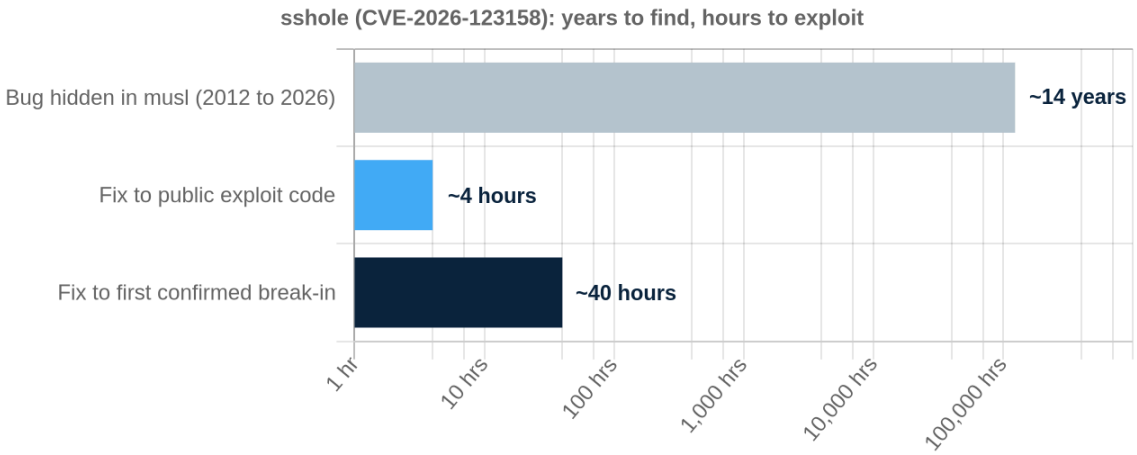

*Figure 8. *sshole timeline, in hours on a log scale. The 40 hours is GreyNoise's first confirmed exploitation; other firms reported break-ins within about a day. Sources: Kültekin (2026); BleepingComputer (November 9, 2026).*

AI models are a component no advisory covers. MONAI, the main open-source framework for medical imaging AI, had three High-severity (8.8) flaws in September 2025[12] that let a malicious model or checkpoint file run code when loaded, and a fourth in 2026. About 95% of the malicious models found on Hugging Face in 2024 used the same pickle file format[10]. None of the 42 CISA medical advisories from 2025–2026 involves an AI component, though about three-quarters of FDA's AI-enabled device list is radiology[13], the same area that leads our advisory data.

CISA's medical list now covers an even smaller share of real exposure. Future editions should add "AI/ML component" and "discovery method" fields to the workbook.

SECTION III: CONCLUSIONS AND PREDICTIONS

How likely we think each development is for 2027. Appendix C5 checks the hypotheses from our earlier editions against this year's data.

LIKELY **CISA's medical advisory list understates real risk**

Manufacturers stopped reporting flaws from their own testing, and large manufacturers publish elsewhere.

LIKELY **Imaging and open-source libraries stay the front line in 2027**

A few DICOM and HL7 libraries sit inside many products.

LIKELY **Home-use devices keep growing as a share**

Consumer and wellness products often sit outside Section 524B.

LIKELY **AI-assisted discovery drives a jump in imaging and open-source disclosures**

Open-source DICOM code is already being swept and maintainers are falling behind, though CISA may publish only a fraction.

PLAUSIBLE **Vendor responsiveness becomes a regulatory issue**

FDA's postmarket cybersecurity draft (FY2027 list) and QMSR inspections are taking hold.

PLAUSIBLE **The first CISA medical advisory for an AI component, such as a model loader or framework**

As soon as 2027. MONAI already has High-severity CVEs, and most FDA AI-enabled devices are imaging products.

POSSIBLE **Code defects overtake authentication**

Within two years, if the 2025–2026 trend holds.

ABOUT MEDCRYPT

Medcrypt helps medical device manufacturers build and maintain secure products, from design through postmarket. Medcrypt Security Intelligence brings threat modeling, SBOM and vulnerability management, and submission documentation into one platform, so product security, regulatory and quality teams can meet FDA, EU and Health Canada expectations with less manual work.

Want to talk through what this data means for your products? Reach out at info@medcrypt.com.

APPENDIX A: METHOD

- **2013–2024:** Medcrypt's hand-coded workbook.
- **2025–2026:** coded by Claude to the same columns.
    - **Root cause:** uses the workbook's most common coding for each CWE already seen. 23 new CWEs were coded fresh.
    - **Other fields:** device type, category, care setting and patch status were read from each advisory.
    - **Review:** flagged in the companion workbook for analyst review.
- **Researcher credit:** CSAF acknowledgments, checked by hand.
- **Large manufacturers:** MDDI top-40 list. 2017–2024 counts follow Mike Kijewski's UCSD analysis.

APPENDIX B: ADVISORIES

The vulnerability-level data behind this report, as published by CISA (527 vulnerabilities in 202 advisories, 2013–2026), is available as a public spreadsheet: CISA Medical Advisory Data 2013–2026.

APPENDIX C: SUPPORTING DATA

C1. ADVISORIES BY YEAR

Year	Advisories	Vulnerabilities	Manufacturer self-reported	Patch available	Large-manufacturer advisories
2017	16	33	8	69%	12
2018	31	70	9	55%	26
2019	20	40	5	55%	18
2020	24	85	7	58%	20
2021	19	89	5	74%	15
2022	15	26	7	33%	11
2023	10	26	5	80%	7
2024	13	27	4	77%	6
2025	24	57	0	83%	3
2026*	18	37	0	67%	0

Through Nov 13, 2026. Workbook years include a small number of ICSA (non-medical-ID) advisories on medical products. Patch status uses one rule for all years (see the notes under C2).

C2. WHO IS DISCLOSING, AND HOW ATTACKS REACH DEVICES

Measure	2013–16	2017–20	2021–24	2025–26
Advisories from first-time vendors	83%	39%	39%	62%
Network-exploitable vulnerabilities (AV:N)	74%	47%	41%	62%
Adjacent/Bluetooth (AV:A)	9%	25%	20%	13%
Physical access required (AV:P)	0%	15%	19%	6%
No privileges required (PR:N)	67%	76%	73%	79%
"Medical device" share of advisories	67%	75%	58%	48%

Who found it matters less than device type. Advisories the manufacturer reported itself had a patch available 56% of the time (2017–2026), against 67% for researcher-found ones. Counting planned fixes, the two are about even (80% vs. 76%).

Mitigation categories grew between 2021–2024 and 2025–2026: the workbook's "vendor unresponsive" category (no vendor response to CISA) rose from 1 advisory to 4, "transition to new product" (end-of-life, no fix) from 1 to 3, and "apply updates, contain physical control" from 1 to 5, driven by home and Bluetooth devices.

Method notes: first-time vendor counts merge spelling variants of the same company (for example "Fujifilm" and "FUJIFILM Healthcare Americas", "B. Braun" and "B.Braun"). Patch status uses one rule for all years, recoded from each advisory's remediation text in CISA's machine-readable (CSAF) files: a patch, update or fixed version was available as of CISA's latest revision. Planned fixes are counted separately in the workbook. Mitigation categories are used only for the newer codes.

C3. CARE SETTING

Year	At home	Both	Hospital (HDO)
2017–2022 (range per year)	0–3	3–5	11–26
2025	4	1	19
2026	5	1	12

C4. DISCLOSURE PROGRAM CHANGES AT THE TOP 40

Five programs got stronger. Zimmer Biomet published a formal CVD policy (June 2025), Hologic became a CNA (May 2026), J&J issued version 2.0 of its CVD statement (July 2026), Solventum set up a security hub after its 3M spin-off, and Dexcom added a CVD program, advisories and a trust center. Two went the other way: Fujifilm's healthcare business no longer lists a security contact, and we found no channel for Cardinal Health. Several advisory lists have gone stale, with nothing newer than late 2023 or early 2024 at Abbott, Edwards, Hologic, bioMérieux and J&J.

C5. EARLIER HYPOTHESES, REVISITED

1. Third-party libraries will be referenced less often

VERDICT: SUPPORTED, WITH A TWIST

Third-party library root causes fell from 8% of vulnerabilities (2013–2016) to 0% (2025–2026). But open-source libraries now appear as the advisory vendor themselves, with 8 advisories for open-source DICOM projects in 2025–2026, so the risk moved into the supply chain instead of going away. AI frameworks such as MONAI are the next layer (Part 3).

3. Reports are limited to the basics; as manufacturers mature, disclosures will rise sharply

VERDICT: NOT SUPPORTED

Advisories stayed at 10 to 30 a year, top-40 manufacturer advisories fell to zero, and the basics (authentication and code defects, 80% of vulnerabilities) still dominate.

4. Mitigations won't be meaningful beyond patching, and patches will take more than six months

VERDICT: PARTLY SUPPORTED

67–83% of recent advisories include a patch, and the rest rely on network controls or vendor contact. Time to patch can't be measured from public data. The median time from first publication to last revision for updated advisories was 79 days (2017–2020), 116 days

(2021–2024) and 42 days (2025–2026, only 6 advisories). Exploitation now comes in days, not months (*sshole, Part 3).

5. Disclosures will settle at a steady rate per quarter for top-40 vendors

VERDICT: NOT SUPPORTED

Top-40 advisories went from about 6.5 a quarter (2018) to 0.75 (2025) and 0 (2026). They didn't level off; they moved to company portals or stopped.

Hypothesis 2 (Medcrypt addresses more vulnerabilities than are reported) needs the "Addressed by MedCrypt Today?" coding, which stops at 2024.

SOURCES AND ENDNOTES

1. CISA, ICS Medical Advisories (ICSMA), CSAF repository, github.com/cisagov/CSAF, accessed November 13, 2026.
2. CISA, Known Exploited Vulnerabilities Catalog, release of November 13, 2026, cisa.gov/known-exploited-vulnerabilities-catalog.
3. Medcrypt, ICS-CERT medical advisory assessment workbook, 2013–2024 (hand-coded; extended to 2026 for this edition).
4. M. Kijewski, "Situation 2046," presentation at UC San Diego, 2026.
5. MDDI, Top 40 Medical Device Companies list (definition of "large manufacturer").
6. Manufacturer product security and coordinated vulnerability disclosure pages for the top 40 manufacturers, reviewed November 16, 2026.
7. A. Wirth, "CVSS for Medical Device Product Risk: Flawed, but Still Essential," Medcrypt, October 22, 2026.
8. Boston Scientific, Q3 2026 earnings release (Form 8-K exhibit), October 28, 2026, sec.gov/Archives/edgar/data/0000885725/000088572526000066/earningsrelease_live.htm; Stryker, Form 8-K/A (Item 1.05) on the March 11, 2026 cybersecurity incident, sec.gov/Archives/edgar/data/310764/000119312526149607/d112875d8ka.htm; Medtronic, notice of data breach filed with the California Attorney General, oag.ca.gov/system/files/Consumer%20Letter%20-%20Exhibit%20A%20%281%29.pdf, and company statement updated June 29, 2026, news.medtronic.com/Medtronic-statement-on-unauthorized-system-access.
9. Cloud Security Alliance, research paper on the AI vulnerability disclosure bottleneck, November 6, 2026 (Project Glasswing figures, NVD prioritization, maintainer responses). Discovery figures are self-reported by the programs involved.
10. Cloud Security Alliance, research note on malicious AI model repositories, May 2026 (citing JFrog's March 2024 findings on Hugging Face).
11. Ö. Kültekin, *sshole (CVE-2026-123158) write-up, sshhole.com, November 2026; BleepingComputer, "Hackers exploit SSHole OpenSSH flaw to breach Linux systems," November 9, 2026.
12. Project MONAI CVE records CVE-2025-58755, CVE-2025-58756, CVE-2025-58757 (September 2025) and CVE-2026-21851.
13. FDA, Artificial Intelligence-Enabled Medical Devices list, accessed November 2026.

DISCLOSURES

The authors are employed by Medcrypt, Inc., a medical device cybersecurity software company. Advisory data is public and comes from CISA and manufacturers' own security pages.