

THE MISSING LINK BETWEEN CYBERSECURITY VULNERABILITIES AND PATCHES

An analysis of ICS-CERT cybersecurity disclosures reveals **no correlation** between a vulnerability's CVSS score and the likelihood a patch will be made available by the manufacturer.

Background:

Throughout a software's lifetime, it will run into problems. A patch is the immediate fix to those problems.

In 2016, the FDA released the guidance document entitled Post-Market Management of Cybersecurity in Medical Devices, in which the FDA makes several recommendations to medical device vendors and health-care delivery organizations on how to manage the cybersecurity risk that connected medical devices introduce. One of the recommendations is for device vendors to design devices to "anticipate software patches," in which the design of a device must consider the need for ongoing patching as well as a mechanism to rapidly deploy patches based on identified vulnerabilities.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has played a critical role in bringing visibility to emergent threats by building a repository for medical device manufacturers to communicate with customers. Assessing these alerts for patching attributes revealed a **50%** increase in frequency of patching vulnerabilities since the FDA has issued their guidance document, but no correlation between CVSS scores and frequency of patching but **no correlation** between CVSS scores and frequency of patching.

READERS WILL LEARN

OBSERVATION	PREDICTIONS	FOR ADDITIONAL DETAIL
Regulatory Guidance Requires Patching Consideration in Device Architecting	Additional device vendors and vulnerability types will increase frequency of patching	Section I
Patching is Selectively Used as a Mitigation	Future disclosures across all device types will increase frequency of patching	Section II
Security Researchers Influence Patching	"Bar for patching" will lower, increasing volume of patching	Section III
Frequency of Patching has Increased, but Concentrated in Industry Leaders	Best patching practices will become required to compete in the marketplace	Section IV

A NOTE ON THE INCLUSION OF VENDOR NAMES:

It should be noted that the authors of this paper consider the inclusion of a specific medical device vendor's name in the list of companies below **to be a positive indicator** of their **active management** of cybersecurity risk. No piece of technology is completely devoid of cybersecurity risk, and so any manufacturer of a technology product should be expected to have to deal with managing cybersecurity vulnerabilities in their products from time to time. Medical device vendors who actively disclose and address cybersecurity vulnerabilities should not necessarily be seen as negligent for having a cybersecurity vulnerability, but rather should be applauded for addressing their vulnerabilities publicly.

Patching medical devices informs system architecture designs, including connectivity, clinical and practitioner interaction. If you deal with a connected device, you will benefit from understanding the state of patching today.

SECTION I: MEDICAL DEVICE PATCHING 101


Patching is defined as a fix for a piece of programming that is designed to resolve functionality issues, improve security and/or add new features. Frequently these patches are available from the software maker's website with indications as to whether in the future a more thorough solution will be available as part of a software release.

A security patch is especially important as it addresses a known vulnerability. The active management of patches by medical device manufacturers is an indication of a functioning security program that actively identifies and addresses software vulnerabilities. Collaborating with security researchers is one of several ways to identify vulnerabilities.

No software is ever 100% secure—medical device or otherwise—but the medical device industry has made great advancements over the last decade. The [FDA Postmarket Management of Cybersecurity in Medical Devices - guidance](#) released in December 2016 encourages medical devices be patched and updated on an ongoing basis. This may lead to the question, *what is different about patching in medical devices vs. other internet of things (IoT) solutions?*

In the medical device world the stakes can be much higher than security on a household thermostat. An unpatched medical device can lead to a patient safety concern and/or patient data being put at risk. But at the same time, the update process itself can introduce potential risks.

To be clear, we are not saying patching is a panacea for medical device vulnerabilities. There are several reasons, thinking in particular of embedded devices like pacemakers, where it may be impractical to deploy patches. Unpredictable connectivity, clinical up-time requirements and prolonged device lifespans are a just a few reasons why patching can be especially challenging in medical devices. However, for many devices and vulnerabilities patching is an effective mitigation and this paper examines the data associated with these.



NO SOFTWARE IS EVER 100% SECURE —MEDICAL DEVICE OR OTHERWISE— BUT THE MEDICAL DEVICE INDUSTRY HAS MADE GREAT ADVANCEMENTS OVER THE LAST DECADE.

SECTION II: DATA

Previous assessments of the [ICS-CERT Advisory Database](#) have indicated the pace of disclosures has grown nearly 400% quarter over quarter since the FDA issued the Postmarket Management of Cybersecurity in Medical Device Guidance (December, 2016). Similarly—the number of vendors participating in the disclosure community has also increased more than 400% since the guidance was released, indicating active and intentional product security teams.

To better understand what happens after a vulnerability has been disclosed, the mitigations were assessed to determine whether patches or software upgrades were made available. A Google Sheet spreadsheet with the data we've extracted from these advisories can be found [here](#).

VULNERABILITY DISCLOSURE FREQUENCY

Subsequent to the FDA postmarket guidance being issued, the frequency of patched vulnerabilities increased by 46.5%—with 75.2% of vulnerabilities since the FDA guidance including device patching as part of the vendor mitigation response.

	Oct. 2013 – Dec. 28, 2016	Dec. 29, 2016 – Aug. 8, 2019
Number of Advisories	12	56
Total Vulnerabilities Disclosed in Advisories	37	117
Average Vulnerabilities Per Month	.95	3.65
Companies (Number of Advisories)	Total:6 Animas, Baxter, Carefusion (2), Hospira (5), Philips (2), Smiths Medical	Total: 23 Abbott Laboratories (2), B. Braun, BeaconMedaes (3), Becton, Dickinson and Company (8), Biosense Webster Inc. / Johnson & Johnson, BMC, Boston Scientific, Carestream, Change Healthcare, Dräger, Ethicon Endo-Surgery / Johnson & Johnson, Fujifilm, GE (2), i-SENS, Medtronic (8), Natus Medical, Inc., Philips (15),Qualcomm Life, Roche, Siemens (2), Silex Technology/GE Healthcare, Smiths Medical, St. Jude, Stryker, Vyair
Mean Vulnerabilities CVSS Score¹	7.3	6.77
Percentage of Vulnerabilities with Mitigation of Patching Devices	51.4%	75.2%

¹ CVSS transitioned from version 2.0 to version 3.0 during the period from October 2013 to December 28, 2016, the negligible impact of which has been assessed as part of [Appendix A](#).



SUBSEQUENT TO THE FDA POSTMARKET GUIDANCE BEING ISSUED,
THE FREQUENCY OF PATCHED VULNERABILITIES INCREASED BY 46.5%

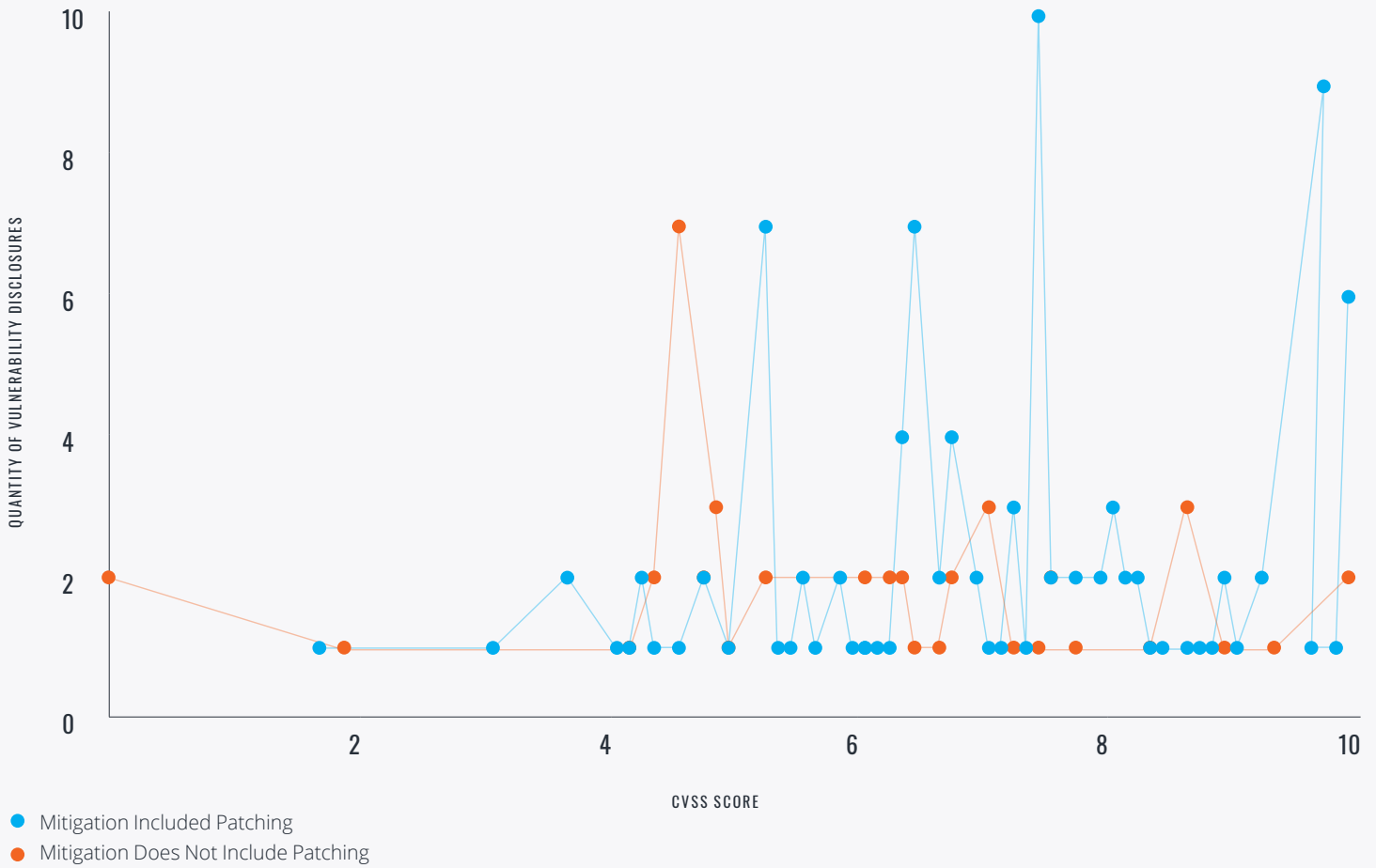
PATCHING AND CVSS SCORES

The CVSS score attributed to a vulnerability is frequently discussed—whether by the media or as an indicator of the impact of a vulnerability on a device. In reality, understanding a vulnerability requires a more nuanced view of what a CVSS score includes. For example, knowing the relationship between a CVSS and exploitability of a vulnerability in its actual use environment can offer insight into whether a high CVSS score actually has a low level of exploitability in the context of the environment in which it operates. Equally important is knowing what a CVSS score does not say—it doesn't identify what network security looks like nor what an attacker could be looking for.

With that in mind, one of the attributes we considered was whether the frequency with which patching was recommended as a mitigation had a relationship to the CVSS scores of vulnerability disclosures.

Thinking the vector string—which influences CVSS scores—may offer additional insight, the 90 unique vector strings in the vulnerability disclosures were reviewed, but no statistically significant concentration of patching was identified. Interestingly, the medium rated vulnerabilities were the least frequently patched (see raw data for why TM1 were excluded from assessment).

EXAMINING THE RELATIONSHIP BETWEEN PATCHING AS A MITIGATION AND CVSS SCORES



VULNERABILITY CAUSES

We attempted to sort the disclosures into seven 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 B](#) for an explanation of each category.)

Attributed Root Cause	Number of Vulnerabilities	Mitigation Included Patching
Code Defect	36	27
Encryption	18	8
O.S. Vulnerability	8	5
System Configuration	18	13
User Authentication Misc	7	5
User Authentication	65	48
Misc	4	1
Grand Total	154	107

SECTION III: OBSERVATIONS ABOUT PATCHING

NO CORRELATION BETWEEN CVSS SCORES AND PATCHING FREQUENCY

CVSS v.3 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.

There are some that state that CVSS is not an accurate measure and [does not account for safety](#). Perhaps the absence of a relationship between frequency of patching and CVSS scores indicates there are other factors considered by device vendors in choosing to patch or not? The data seems to support as greater than 30% of vulnerabilities were not patched.

There are however, facets of the CVSS scoring method which are not used in medical devices (i.e. temporal metric group & environmental metric group). Perhaps if these were incorporated, it may address some of the concerns with the system?

For example the temporal metric group, meant to reflect characteristics that may change over time, includes a measure for remediation level. If this were assessed and whether something is available, can be worked around, temporarily fixed, or officially fixed, could better reflect mitigations. The environmental score, which represents attributes relevant to a particular user's environment, is calculated based on the importance of the affected asset, measured in terms of confidentiality, integrity and availability.

We applaud MITRE which has advocated and outlined the need for an expansion of CVSS that accounts for clinical and patient safety sensitivities. [The Rubric for Applying CVSS to Medical Devices \(January 2019\)](#) and collaboration with the entire healthcare ecosystem, including healthcare delivery organizations (HDO), medical device manufacturers (MDM), security experts and safety experts confirms the importance of measured in terms of confidentiality, integrity and availability.



NETWORK MONITORING AS A MITIGATION

Of the 154 vulnerabilities assessed, 47% of the 107 that included patching recommendations also included a recommendation that deviated from the standard network best practices as part of their recommendations (standard is defined as the NCCIC/ICS-CERT recommendation for network, which includes variations on limiting network exposure, locating devices behind a firewall and using VPN for connectivity). This includes 6 which recommended the device be disconnected from the network, 8 that did not have any network related mitigation, and 24 that explicitly recommended HDOs monitor network traffic.

How does disconnecting a device impact patient experience? Perhaps the risk to update or the clinical circumstances in which these devices operate presented unique challenges in addressing.

SECURITY RESEARCHERS AND PATCHING

Most responsible disclosures follow the same basic steps - a security researcher identifies a vulnerability and potential impact. Documentation of their findings, sometimes including a repeatable proof-of-concept attack, are shared with medical device vendors in the form of a vulnerability advisory report which includes more details of the vulnerability and a disclosure timeline. Researchers then typically allow a vendor reasonable time to investigate and fix an exploit, often resulting in a patch being made available for the researcher to further assess.

Considering some of the more high profile disclosures that have come out, we assessed whether there was a relationship between vulnerability disclosures that referenced a security researcher being patched vs. not. Of the 95 vulnerabilities that included an explicit reference to a security researcher, 69.5% of these included references to patching as part of the mitigation strategy. Risk level did not appear to influence the frequency of patching, but perhaps there is a higher pressure in partnering with researchers to encourage patching as a mitigation?

Attributed Root Cause	Security Researcher Referenced	Mitigation Including Patching	Percentage of Security Researcher Referenced Vulnerabilities that included Mitigation Patching
Low	3	3	100%
Medium	39	24	61.5%
High	39	30	76.9%
Critical	11	8	72.7%
TM1	3	3	100%
Grand Total	95		

SOME COMPANIES LEAD WITH PATCHING

Device type was also considered and found a concentration of 59% of patching associated with imaging software, infusion pumps and diagnostics systems. This was heavily driven by Phillips which issued 20 of the 23 patches associated imaging software. 75.9% of those companies which have participated in coordinated disclosures have issued patches in relation to vulnerabilities disclosed.

In our last whitepaper (October 2018) we noted of those companies who have made disclosures against a list of connected-device vendors ranked by market cap, only seven (7) of the top 29 medical device vendors have ever made a vulnerability disclosure through the ICS-CERT system. As of August 8, 2019 this has increased to 11 device vendors that have issued a disclosure. Of these, 9 vendors have included patching as part of their recommended mitigations.

There are two valid reasons a medical device vendor would never have made a patch available for a device.

- 1 The process of updating a device results in a patient safety concern that cannot be mitigated
- 2 Updates sent to medical devices cannot be authenticated and therefore remain unapplied

The [FDA Premarket Submissions for Management of Cybersecurity in Medical Devices](#), which reflects the FDAs current thinking—even in draft form—indicates that proactively considering how updates/patches are administered to medical devices is critical to the continued security of a device.

Regardless of the reason for the update, devices that are secure will have been designed with consideration for ongoing security maintenance. This means software and hardware are developed with updates in mind—specifically ensuring there is a secure mechanism for software updates. Whatever the mechanism of choice is, medical device operational considerations—like a loss of communication (network connectivity) or loss of power during an update—should be built into a fault-tolerant process.

Those devices that support critical life functions and/or have lower computing capability (like a pacemaker), must have an update mechanism that minimizes downtime and uses limited resources. Clinical use cases must also be considered. While an automatic update can work for a non-critical system such as a coffee maker, there have been instances where life-sustaining devices were updated without concern for patient use. Designing the process for triggering updates, developing authorizations to confirm the validity of an update and timing the update should be built into how a device operates.

A proactive approach towards security software updates will avoid substantial headaches after a device is released and ensure that medical devices receive updates to improve functionality, protect patient safety and data security and maintain operational requirements with other devices.

LEAST FREQUENTLY PATCHED

The highest concentration of vulnerabilities least frequently patched were infusion pumps from a single device vendor in 2015. *Is this attributed to the sheer volume of pumps operating in hospitals?* Or perhaps this demonstrates a maturity in security management over time. Pumps frequently operate in both hospital environments (i.e. where networks are actively managed) as well as in mobile units/at home (which can rely on alternate connectivity mechanisms). Perhaps timing is the most obvious cause—this was prior to the FDA premarket guidance being released. There was a reliance on alternative compensating controls, specifically network monitoring, which at the time may have been more readily accepted in the community.

There are also fewer patches due to vulnerabilities in third-party libraries than we would expect. For example, OpenSSL, a widely-used open source encryption library, had **34 CVE** vulnerability reports in **2016 alone**, resulting in **13 software patches** across OpenSSL versions 1.0.1, 1.0.2, and 1.1.0. Given OpenSSL's relative ubiquity in today's enterprise software, it's likely that dozens or hundreds of medical devices are running deprecated versions of OpenSSL with known vulnerabilities. **Yet we see no examples of medical device vendors including references to OpenSSL vulnerabilities in even a single ICS-CERT advisory.** It could be that vendors are patching these vulnerabilities regularly, but they are not seen as critical enough to warrant an ICS-CERT advisory. As seen in non-medical device advisories, it may be helpful for these patches to trigger advisories so other device vendors see the frequency with which vendors are patching vulnerable open source libraries.

SECTION IV: HYPOTHESES AND PREDICTIONS

WannaCry was an example where an **estimated 98%** of the infected devices were running Windows 7, for which a patch was released 7 months before the attack hit. Medical devices present practical circumstances that ensure solving patching in isolation is not sufficient. The complexity of medical device security is the challenge here.

Looking at the entire ecosystem, if the average hospital bed has **10-15 devices** connected to it and the American Hospital Association estimates there are about **900,000** hospital beds in 2019, there are at least 9,000,000 devices inside U.S. hospitals. Will the industry ever be able to patch fast enough and complete enough? The future of medical device security is proactive healthcare security that is designed into a devices while focusing on clinical use cases and patient safety.

CVSS scores do not correlate to frequency of patching of vulnerabilities.	The industry will decide on a framework / criteria to determine which vulnerabilities are consistently patched.
Patching in isolation does not sufficiently address device vulnerabilities.	Proactively secure devices that have security designed into them will be more resilient to vulnerabilities and able to tolerate a delay in patch deployment.
Many medical device vendors are only recently beginning to prioritize cybersecurity as part of their Engineering, R&D, and Quality processes.	The list of medical device vendors who are participating in ICS-CERT cybersecurity disclosures will grow significantly in the coming three years, and will begin to include names of vendors who are not in the "top 30".
Stigma surrounding the patching of cybersecurity vulnerabilities has historically caused vendors to be reluctant in issuing updates to devices.	The FDA's continued advocacy for patching, and leading medical device vendors competing on security in the marketplace, will drive added participation by all device vendors
The industry has begun to address the "low hanging fruit" of medical device cybersecurity, but has yet to address more deeply technical causes of vulnerabilities at scale.	The complexity of vulnerabilities disclosed via ICS-CERT will steadily increase. As vendors work through their portfolios to eliminate things like hard-coded user-names and passwords, more fundamental flaws in system design, like the inability to apply patches, will take focus.

DISCLOSURES

The authors of this paper are employed by MedCrypt Inc, a medical device cybersecurity software developer.

Thank you.

Mike Kijewski, CEO
mike@medcrypt.com

Axel Wirth, CSS
axel@medcrypt.com

Vidya Murthy
vidya@medcrypt.com

APPENDIX A

ASSESSMENT ON CVSS VERSION IMPACT

CVSS transitioned from version 2.0 to version 3.0 during the period from October 2013 to December 28, 2016, the details of which are outlined in [Table 1: CVSS v2.0 to v3.0 Changes](#).

The advisories under review were bucketed into qualitative ranges based on the [NVD criteria](#) outlined below. 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.

CVSS V3 RATINGS

- 1 Vulnerabilities are labeled “Low” severity if they have a CVSS base score of 0.0-3.9.
- 2 Vulnerabilities will be labeled “Medium” severity if they have a base CVSS score of 4.0-6.9.
- 3 Vulnerabilities will be labeled “High” severity if they have a CVSS base score of 7.0-8.9.
- 4 Vulnerabilities will be labeled “Critical” severity if they have a CVSS base score of 9.0-10.0.

CVSS V3 RATINGS

- 1 Vulnerabilities are labeled “Low” severity if they have a CVSS base score of 0.0-3.9.
- 2 Vulnerabilities will be labeled “Medium” severity if they have a base CVSS score of 4.0-6.9.
- 3 Vulnerabilities will be labeled “High” severity if they have a CVSS base score of 7.0-10.0.

	Critical	High	Low	Medium	TM1	Grand Total
Post - FDA	13	27	2	42	1	85
Pre - FDA	1	19	1	13	3	37
Grand Total	14	46	3	55	4	122

The assessment of the new version by Omar Santos, Cisco, predicted in *'The Evolution of Scoring Security Vulnerabilities'*, an increase in high and critical findings under version 3. The medical device advisories demonstrated a shift in more medium categorizations between version 2 and 3 (see table below). This may be an indicator that even with an increase in vulnerabilities reported, the reported vulnerabilities were lower risk, perhaps further corroborating alignment with fewer technical findings.

	Version 3 Count	Version 3 Percentage	Version 2 Count	Version 2 Percentage
Critical	14	16%		
High	28	31%	17	61%
Medium	45	51%	10	36%
Low	2	2%	1	4%

Specifically as outlined in [Table 3](#), the common vulnerabilities (CWE IDs) anticipated to cause increases are buffering and user authentications, which are notably attributed as the root cause for many of the medical device advisories.

APPENDIX B

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.

Miscellaneous: Disclosures that did not fit into one of the above categories were labeled “Miscellaneous.”