PROACTIVE HEALTHCARE CYBERSECURITY

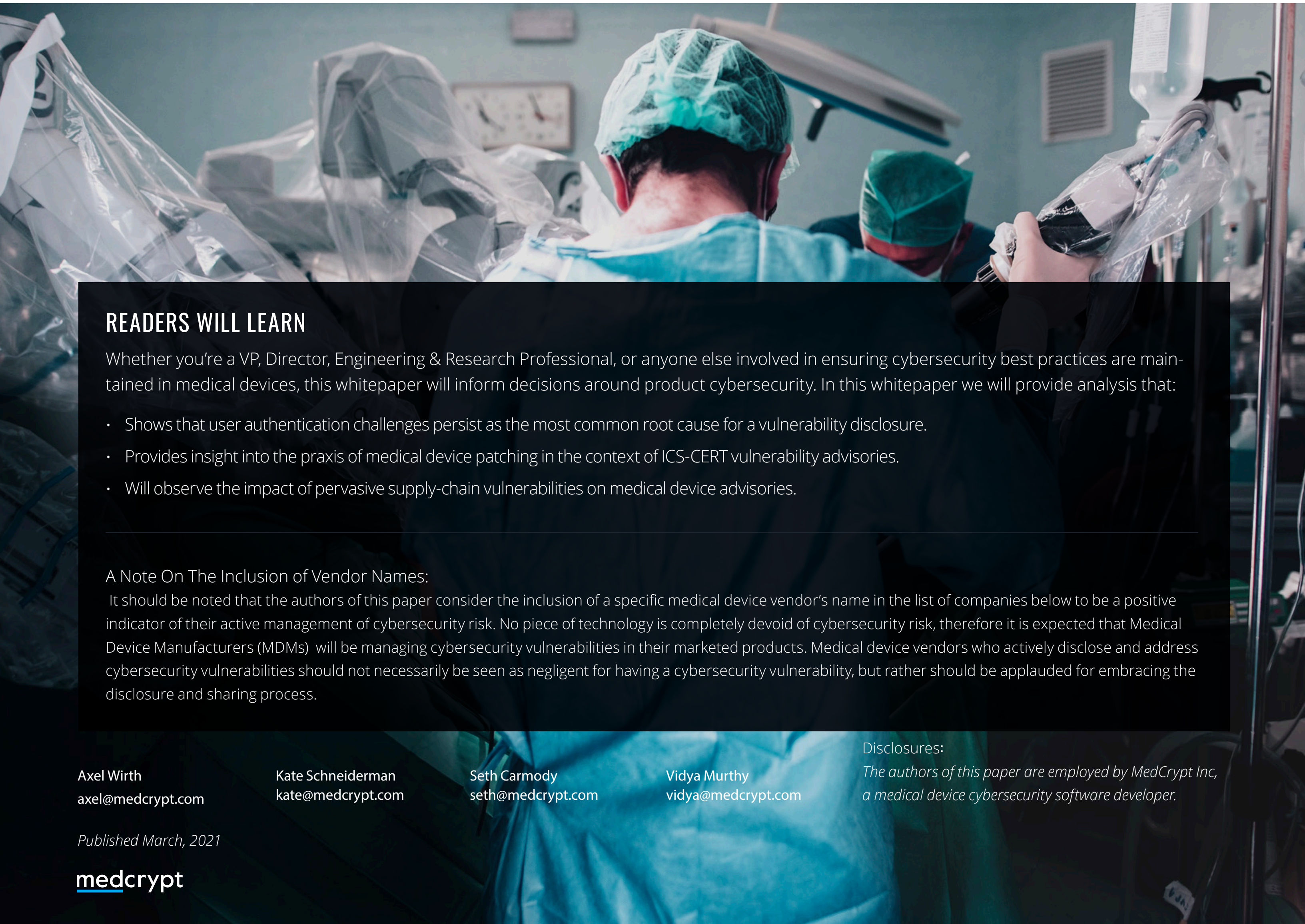
WHAT THE MEDICAL DEVICE INDUSTRY CAN LEARN FROM PAST CYBERSECURITY VULNERABILITY DISCLOSURES

Since FDA released their Postmarket Cybersecurity Guidance in 2016, the monthly rate of ICS-CERT medical device advisories disclosed has increased 6.4-fold.

Background:

In December 2016, the FDA released a guidance document entitled Postmarket Management of Cybersecurity in Medical Devices, in which the FDA makes several recommendations to medical device vendors and healthcare delivery organizations on how to manage the cybersecurity risks introduced by connected medical devices . One of the recommendations is for device vendors to participate in cyber risk information sharing, in which information about security vulnerabilities is shared with the medical device community via Information Sharing Analysis Organizations (ISAOs). A medical device cybersecurity advisory issued by ICS-CERT can be the result of either self-reporting by the vendor or from a third party, like a researcher, via an ISAO or directly to ICS-CERT.

*This is an updated version of our original 2018 whitepaper analyzing trends in cybersecurity vulnerability disclosures.



READERS WILL LEARN

Whether you're a VP, Director, Engineering & Research Professional, or anyone else involved in ensuring cybersecurity best practices are maintained in medical devices, this whitepaper will inform decisions around product cybersecurity. In this whitepaper we will provide analysis that:

- Shows that user authentication challenges persist as the most common root cause for a vulnerability disclosure.
- Provides insight into the praxis of medical device patching in the context of ICS-CERT vulnerability advisories.
- Will observe the impact of pervasive supply-chain vulnerabilities on medical device advisories.

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, therefore it is expected that Medical Device Manufacturers (MDMs) will be managing cybersecurity vulnerabilities in their marketed products. 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 embracing the disclosure and sharing process.

Axel Wirth
axel@medcrypt.com

Kate Schneiderman
kate@medcrypt.com

Seth Carmody
seth@medcrypt.com

Vidya Murthy
vidya@medcrypt.com

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

Published March, 2021

SECTION I: DATA

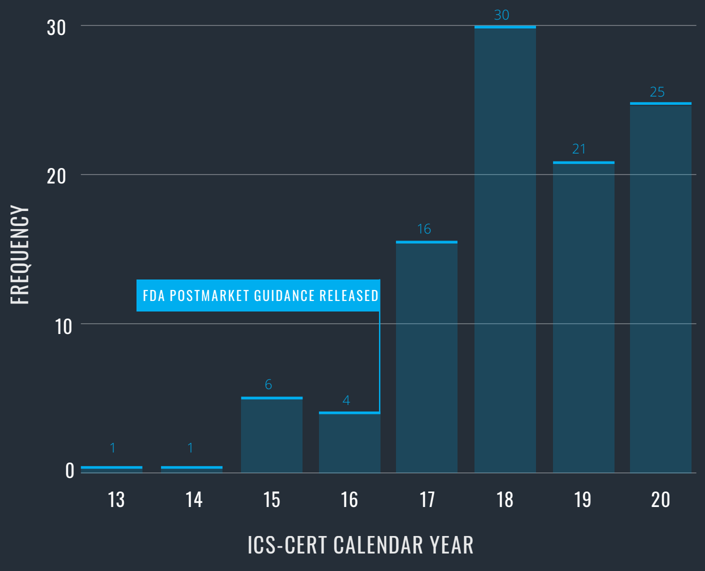
The ICS-CERT Advisory Database was analyzed to identify all advisories related to medical devices. In total, 104 advisories were released between October 2013 (issuance of the first ICS-CERT medical device advisory) and December 2020, consisting of a total of 269 individual cybersecurity vulnerabilities. Advisories were extracted and divided into two time frames—before and after the FDA Postmarket Management of Cybersecurity in Medical Device Guidance (which was finalized for implementation on December 28, 2016).

VULNERABILITY DISCLOSURE FREQUENCY

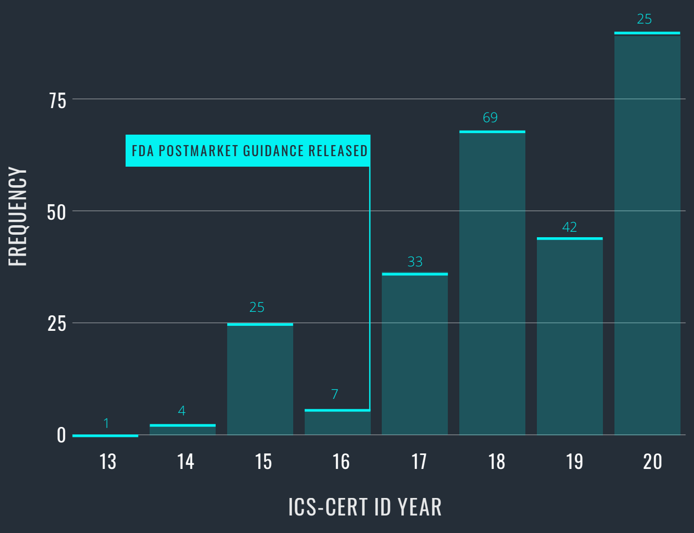
	Oct. 2013 – Dec. 2016	Jan. 2017 – Dec. 2020
Number of Advisories	12	92
Total Vulnerabilities Disclosed in Advisories	37	232
Average Advisories per month	0.31	1.92
Average Vulnerabilities per month	0.95	4.83
Companies (advisories issued)	Animas, Baxter, Carefusion (2), Hospira (5), Philips (2), Smiths Medical	Abbott Laboratories (2), B. Braun (3), Baxter (5), BeaconMedaes, Becton, Dickinson and Company (11), Biosense Webster Inc. / Johnson & Johnson, BIOTRONIK, BMC, Boston Scientific, Carestream, Change Healthcare (2), Dräger, ENEA/Green Hills Software/ITRON/IP Infusion/Wind River, Ethicon Endo-Surgery/ Johnson & Johnson, Fujifilm, GE (5), Insulet, i-SENS, Medtronic (12), Natus Medical, Inc., OpenClinic GA, Philips (26), Qualcomm Life, Roche, Siemens (2), Silex Technology/GE Healthcare, Smiths Medical, Spacelabs, St. Jude, Stryker, Vyaire
Mean Vulnerabilities' CVSS Score	7.30	6.86[1]

[1] For the period prior to the FDA Guidance ICS-CERT used a mix of CVSS version 2 and 3, and for the period after the guidance document was released, ICS-CERT consistently used CVSS version 3.

ADVISORY FREQUENCY VS. ICS-CERT CALENDAR YEAR

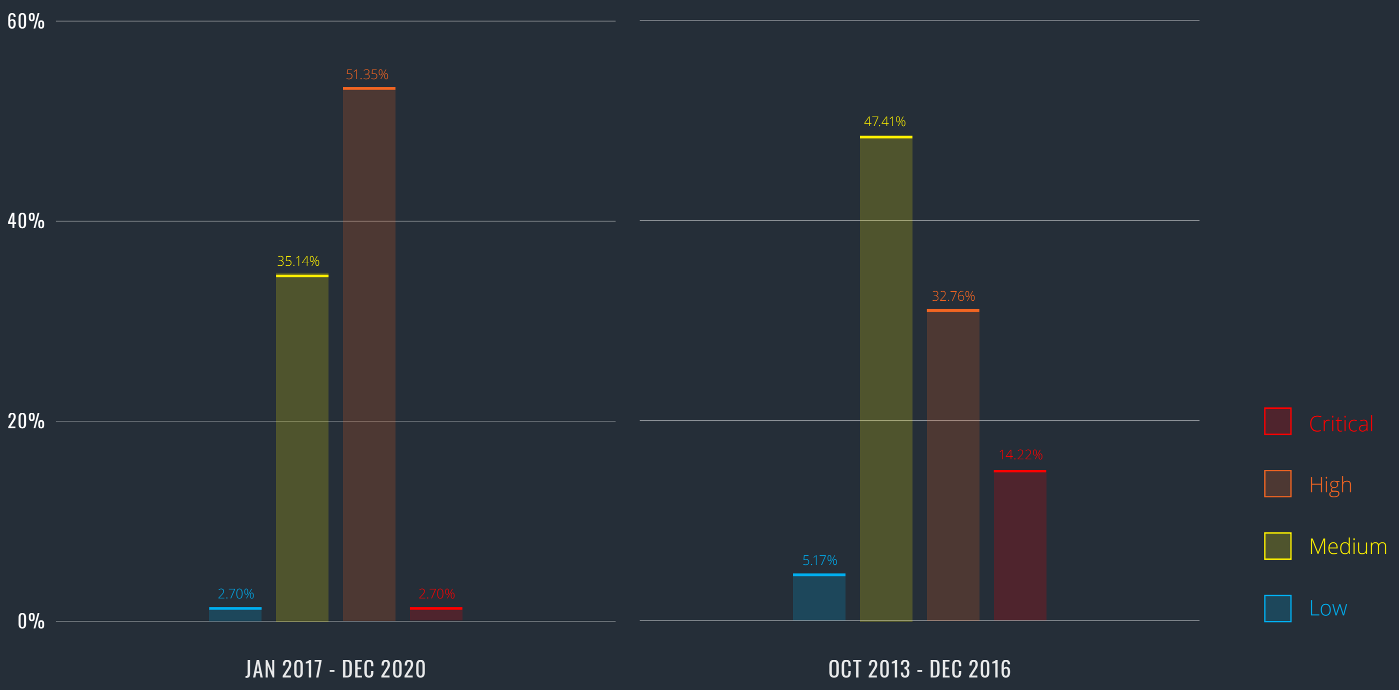


VULNERABILITY FREQUENCY VS. ICS-CERT ID YEAR



Despite not mandated by law, the number of published vulnerabilities has increased since the release of the FDA Postmarket Guidance, with an average of 4.83 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 A, the severity of vulnerabilities were expressed as a percentage of the total vulnerabilities disclosed for a time period. The timing of FDA guidance demonstrates a pivot point after which there was a large increase in critical & medium risk disclosures, along with a decrease in high risk vulnerabilities disclosed. This is particularly impressive since there is no specific disclosure law for MDMs, which means that MDMs view guidance and other factors as market incentives.

ADVISORY RATING ASSESSMENT PRE- & POST- 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.

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 B for an explanation of each category.)

Attributed Root Cause	Oct 2013-Dec 2016 Totals	Jan 2017-Dec 2020 Totals
Code Defect	13% (5)	18% (41)
Encryption	22% (8)	11% (25)
O.S. Vulnerability	3% (1)	10% (23)
System Configuration	11% (4)	13.5% (31)
Third Party Library	8% (3)	2% (5)
Third Party Encryption		0.5% (1)
User Authentication	43% (16)	43% (99)
Misc		3% (7)
Grand Total	100% (37)	100% (232)

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 researchers' 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.

ADVISORIES WHERE A RESEARCHER IS EXPLICITLY REFERENCED

	Post - FDA	Pre - FDA	Grand Total
No	30	1	31
Yes	62	11	73
Grand Total	92	12	104

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.

MEDIAN[2] CVSS VALUE

Root Cause	Post - FDA	Pre - FDA
Code Defect	7.0	7.7
Encryption	6.3	6.1
Misc	5.5	N/A
Operating System Vulnerability	7.8	7.0
System Configuration	6.0	6.5
Third Party (Encryption)	5.3	N/A
Third Party Library	7.4	8.4
User Authentication	7.0	7.9

[2] 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.

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, it 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 in 2020.

ADVISORIES THAT LIST PATCHING AS A MITIGATION

	No	Yes
Post - FDA	50	182
Pre - FDA	18	19
Grand Total	68	201

PREVALENCE OF BROAD IMPACT VULNERABILITIES

Since the disclosure of the EternalBlue vulnerability led to the WannaCry malware events in 2017, we have seen an increase in the reporting of high profile, highly pervasive vulnerabilities. Names like Ripple20, Urgent/11, or Amnesia33 have made the headlines and have sent device manufacturers and healthcare providers scampering to determine which of their devices are at risk. What these vulnerabilities have in common is that they contain a complex collection of a subset of individual vulnerabilities of varying risks, and that they are deeply embedded in our software technology supply chain, often for many generations of a product.

Vulnerabilities affecting the operating systems, hardware components like memory controllers and CPUs, Bluetooth interfaces, and various TCP/IP network stacks have been disclosed, all of which are readily used across the healthcare ecosystem.   The prevalence of these types of deeply embedded supply chain vulnerabilities would suggest an increase in device or technology-specific disclosures by MDMs. However, there has been no demonstrated impact on ICS-CERT advisories because of broad impact vulnerabilities. This isn't to say that MDMs did not discuss these pervasive vulnerabilities, just that the ICS-CERT process is not what was used to do so. In fact, 14 of the top 40 MDMs (by revenue) have a specific reference on their website to at least one of these high impact vulnerabilities that occurred in 2020, with 11 of 12 of those impacted devices referencing a mitigation strategy.

There does seem to be one vulnerability in 2019 that stood out as being unique, ICSMA 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.

SECTION II: OBSERVATIONS ABOUT DISCLOSURE FREQUENCY

THERE ARE MORE VULNERABILITIES DISCLOSED PER ADVISORY

Since 2016, there were 7.7X as many advisories disclosing 6.3X as many vulnerabilities. 2020 averaged 3.5 vulnerabilities per advisory, 2017 through 2019 were approx 2 vulnerabilities per advisory.

There are a couple of possibilities to explain this:

- MDMs are intentionally bundling vulnerabilities together to have fewer advisories due to the increase in pervasive and complex third-party software vulnerabilities with broad impact, or
- that vulnerability management and disclosure practices are improving.

As noted above, the impact of pervasive and critical vulnerabilities (such as Urgent/11 or similar) has been nearly negligible on ICS-CERT disclosures, so that is unlikely to have caused the increase. Therefore, it seems evident that vulnerability disclosure procedures have matured.

There's no good way to know the universe of total vulnerabilities and whether it is increasing, decreasing, or staying the same. However, the increase in disclosures is most likely due to the incentive structure within the FDA's postmarket policy and support of security researchers and the resulting catalytic effect on the maturation of MDMs' internal processes of disclosure.

SOME COMPANIES HAVE YET TO ISSUE AN ADVISORY

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, 17 (13 in 2019) have a published vulnerability disclosure process, which includes both a mechanism to intake feedback and communicate findings. Therefore 19 top medical technology vendors that have connected devices in their portfolio have never made a disclosure through ICS-CERT[3]. Further, of the 92 advisories since December 2016, almost half (49/92) came from 3 companies alone (BD, Medtronic, Philips), demonstrating a high degree of disclosure and postmarket vulnerability handling maturity with these organizations.

There are at least three plausible reasons 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 5 do not offer a product that is computerized nor connected.

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 therefore it is reasonable to assume that some MDMs simply contact their customers directly rather than putting out full public disclosures. Connecting with every customer at network speed however remains an unsolved problem.

   Of those 17 with disclosure processes, three have not made a vulnerability disclosure through the ICS-CERT database. Having a disclosure policy is seen as the crawl step of a maturing process, with the idea that you have the welcome mat for researchers and have the processes in place before receiving a vulnerability report from an external source; therefore, having a disclosure policy and having not used it are still positive signs.

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.

ROLE OF RESEARCHERS

Of the 104 advisories assessed, 73 explicitly referenced a researcher being involved in the identification of the vulnerability. Historically, researchers have been viewed as adversaries, but their attribution to 70% of the advisories assessed confirms their positive presence in the ecosystem. There is no mandate to report vulnerabilities through the Department of Homeland Security (DHS), but through ICS-CERT, DHS has served as mediator through a process which can be fraught with threats of litigation to the researchers. Therefore, it makes sense that the majority of disclosures reference researchers, and perhaps more impressive that MDMs , despite the absence of a legal mandate, continue to self-report vulnerabilities.

[3] This analysis did not comprehensively look at MDM product security website communications

USER AUTHENTICATION IS A COMMON PROBLEM

Vulnerabilities attributed to user authentication and code defects covered 60.4% of the vulnerabilities included in the ICS-CERT advisories after January 1, 2017, a statistically insignificant decrease from 62.5% prior to FDA Guidance in December 2016. This seems indicative of a historical way of working in healthcare assuming trust in the operator of a device. Having a seamless user experience not impeded by additional authentication steps enables enhanced care, which can result in security being a secondary requirement or worse-case, security features could interfere with care delivery .

Perhaps we need to reconsider how device users interact with security features? Instead of the common retort that 'people are the weakest link' perhaps we can better design layers of security into our device to proactively limit the burden on an end user?

ONLY 21.5% PERCENTAGE OF ADVISORIES DID NOT ADDRESS PATCHING

Prior to the FDA postmarket guidance, the frequency of patching being referenced in an advisory was 51.4%. Since then, it is up to 78.5%, which is fantastic progress and should be commended.

But what happens once a patch is available? If we look at today's approach, there are practical restraints on the healthcare delivery organization (HDO) side that limit the effectiveness of medical device security programs. 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, a worthwhile effort but still limited in effectiveness and impact.

Currently, there are significant barriers to implementing patches in the HDO, once they have become available from the MDM. Primarily, that the device may be in use for extended periods, or that the device is actually managed by the MDM or third party servicer. Both of which could contribute to significant delays between disclosure, patch issue, and patch implementation. 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 with the current approach we won't be able to patch fast enough and complete enough to become secure enough.

THE FUTURE OF HEALTHCARE RELIES ON CONNECTED DEVICES, WORKING TOGETHER

medcrypt

SECTION III: CONCLUSIONS/PREDICTIONS

LOOKING BACK

We started reviewing these disclosures in 2018, trying to find data to empirically assess the state of the industry. Some of our prior predictions about the pace of change have unfortunately been confirmed as, in many ways, healthcare cybersecurity is still quite nascent and will need to continue to mature.

As we predicted in our initial whitepaper, we are still in the beginning of maturing vulnerability disclosures. The multi-fold increase in frequency of vulnerability disclosures indicates momentum building, but not nearly at the pace we anticipated. Unfortunately, where we envisioned an opening and sharing of devices with the researcher community, the ecosystem is still missing those devices that aren't readily accessible to researchers. And where devices are available to researchers, low complexity vulnerabilities continue to dominate. This may be taken as evidence of more complex underlying issues, but this has not been substantiated by vulnerability disclosures.

While we had hoped the high-bar for disclosing would rapidly diminish, it has persisted with a couple of potential root cases: 1) internal pressure in an MDM or 2) negative media coverage. Both seem to be attributed as culprits for continued reluctance, even in those MDMs that have leadership which understand the importance of device based cybersecurity and especially vulnerability communication.

And finally, we observed that a non-insignificant population of MDMs do not participate in self-reporting. Perhaps this is because there is no clear value added to the HDO marketplace. Does posting a vulnerability in ICS-CERT enable an HDO to know how to respond to a pervasive vulnerability discovered (e.g., Urgent/11)? Arguably, disclosures are solving a subset of the pain point, but not making it especially usable to the ultimate consumer.

A few years on, it seems appropriate to ask critical questions on progress, impact on the ecosystem, and whether the healthcare industry has been able to find its "true north."

PATH FORWARD:

With the exception of a few MDMs, the majority of ICS-CERT vulnerability disclosures are researcher-driven. Given the relationship between healthcare providers, MDMs, researchers, and regulators, we have to think about whether security research-driven vulnerability disclosures sufficiently scale to lead our industry to a security steady-state.

Certainly ICS-CERT and FDA have given researchers a voice and that needs to continue, not just to avoid negative press from a device hacking presentation or headline, but for product development improvement. It is a standard practice to reuse code when developing a medical device to support clinical functionality. This can mean security debt, such as the lack of authentication or authorization anti-patterns (e.g. no authentication, hard coded credentials), will continue to be passed down the supply chain. The vulnerability disclosure process serves as a market incentive to re-architect and implement a secure design and fix implementation errors where vulnerabilities have been found.

Hypothesis	Predictions
Believing that all researchers want to optimize for their return on effort spent, there will continue to be an increase in the disclosure of broad, high complexity supply chain vulnerabilities.	Researchers will continue to disclose broad impact vulnerabilities. Supply chain vulnerabilities are typically not covered via ICS-CERT medical device vulnerability disclosures and require idiosyncratic investigations to see if devices are impacted. This is untenable and must be centrally managed to be useful to healthcare providers.
Vulnerability disclosures have helped normalize that security is a continuous process. But vulnerability disclosures have a limit in their ability to drive organizational change that is necessary to design more secure devices. This will require a cultural paradigm shift across all stakeholders and roles, from engineer to executive management.	While we may see increases in numbers of disclosures and vulnerabilities, unless new market forces emerge, the types of vulnerabilities will continue to track with traditional security weaknesses.
Reactive security processes are insufficient for the scope of the problem we are facing.	A proactive, technology-driven strategy for securing devices is critical. This includes designing devices with security over the lifecycle of a device, as well as correlating vulnerability insight with device behavior monitoring to identify usable asset specific insights to HDOs.

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 below. .

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 V2 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.

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.

Timeline Relative to FDA Guidance	Critical	High	Low	Medium	TM1	Grand Total
Post - FDA	33	76	12	119	1	232
Pre - FDA	1	19	1	13	3	37
Grand Total	34	95	13	123	4	269

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	23	16%		
High	47	32%	17	61%
Medium	72	49%	10	36%
Low	5	3%	1	4%

Specifically as outlined in Appendix B, 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.

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.”